CONCEPTS OF MATHEMATICS, SUMMER 1 2014 LECTURE NOTES

SEBASTIEN VASEY

Contents

1. About

These are notes for an introduction to proof-based mathematics given at Carnegie Mellon University in the summer of 2014. The course is over but I aim to keep theses notes (together with the source files) available from my website: `http://math.cmu.edu/~svasey/`.

I thank all the 21-127 students who reported typos and mistakes.

Date: June 30, 2014.

2. Introduction: what is mathematics, what is a proof?

The material in the entire section will be covered in Lecture 1 (tentative).

2.1. **What is mathematics?**

The course is not meant to be about the philosophy of mathematics, but it is important to realize that this question is still far from being understood. There are people whose only job is to investigate and discuss this topic. One should also understand that there cannot be one absolute all-encompassing answer: Mathematics means different things to different people (even to different mathematicians). Here is a (non-exhaustive) sample of possible answers:

- Mathematics is the language of Science.
- Mathematics is the study of patterns.
- Mathematics is the study of topics such as quantity (numbers), structure, space, and change [Wikb].
- Mathematics is the study of what can precisely be argued to be true or false.
- Mathematics is what mathematicians do.
- Mathematics is the subject in which we never know what we are talking about, nor whether what we are saying is true [Rus03, p. 5].
- Etc. See for example [Wika] for more.

Whatever mathematics is, most mathematicians would agree that it involves *explaining* rather than just *describing*. The most highly-valued form of explanation in mathematics is called a *proof*.

2.2. **What is a proof?**

In mathematics, a proof is a very precise *argument* explaining *why* a given statement is true. The argument must be so convincing that its audience (anybody who reads/hears it, including the writer of the proof) has no doubt about the truth of the statement. Concretely, this means that:

(1) The statement that is being proven, as well as every step of the proof, must be *unambiguous*: if there is ambiguity on what the statement even says, how can one agree about its truth? In particular, the proof should be understandable to its audience.
(2) The proof must be *logically sound*: not only must every step be correct, but steps should also be *justified* so that no doubt is left about their validity.
(3) A proof must rely on *common ground* shared by the entire audience: if the audience disagrees on the truth of every single fact,

including whether $1 + 1 = 2$ or $1 = 1$, then there is no hope of convincing it using pure reason. This common ground includes some (hopefully simple) statement whose truth is taken as granted (the *axioms*), as well as the valid rules of logic that can be used in a proof. This common knowledge should (explicitly or implicitly) be made clear in the proof itself.

Remark 2.1. Thus a proof also depends on its audience. For example, a five year-old child needs to be explained why $2 + 3 = 5$, while most adults take this fact for granted. Similarly in mathematics, it is permissible to omit explanations for facts that the reader thinks the audience will have no difficulty believing. However, this often leads to laziness on the part of the writer ("the proof is left as an exercise", "obviously, so and so is true") which in turn leads to mistakes. Words such as "obviously", "clearly", etc. are especially dangerous: if a statement is *really* obvious, then one can omit the qualifier entirely (in the "real world", nobody ever says "clearly, $2 + 3 = 5$").

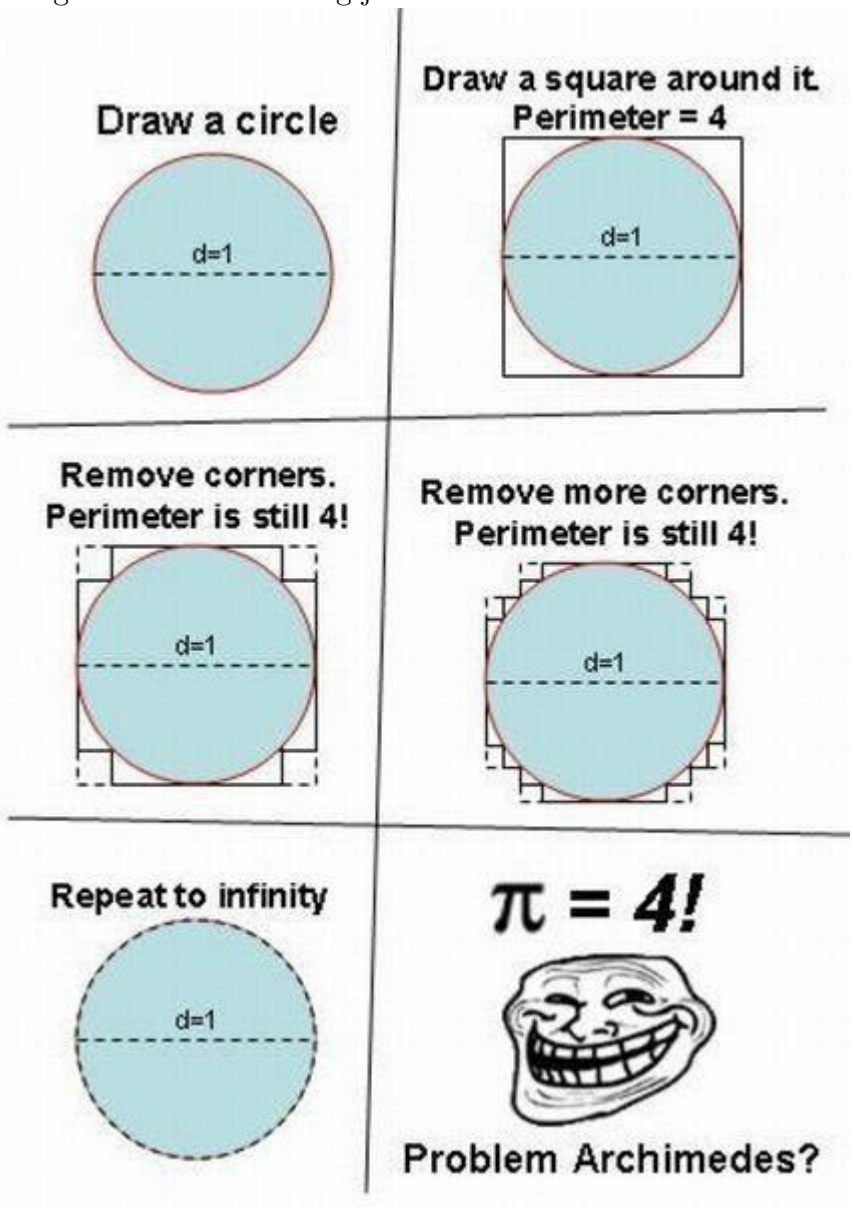
Remark 2.2. On the other hand, there is a danger of writing too many details: this can hurt understanding by burying the most important points of a proof inside pages of easy arguments. A famous extreme case[1] is "Principia Mathematica" [RW25] which takes more than 300 pages to prove that $1 + 1 = 2$ (the statement is accompanied by the comment "The above proposition is occasionally useful"). While leaving no stone unturned, a proof must *emphasize the hard steps*.

We will *not* specify *exactly* what form a proof must take: doing this would force us to impose too many unnatural restrictions, ending up with a programming language-like syntax impossible for humans to work with.

Mathematical proofs can usually be written in plain English, but one must often make use of mathematical symbols to describe something precise that would be too long or too hard to describe in English. Since human languages can be ambiguous, one must often make sure that the argument remains completely clear (additional informal explanations can be marked as such using words such as "intuitively", or "loosely speaking"). On the other hand, writing in plain English improves readability and understandability, so it is advisable to make use of it whenever appropriate. Remember: a mathematician writes for humans, not computers.

[1]Of course, the aim of the authors in writing the book was never to prove to the skeptics that $1 + 1 = 2$, but rather to show that it could in principle be done.

2.3. **Good proofs, bad proofs.** We now consider examples of proofs. We begin with the following joke found on the web[2]:



Needless to say, this argument has several issues. For a start, the conclusion is wrong. However, sometimes even "proofs" for wrong facts

[2] http://s254.photobucket.com/user/balthamossa2b/media/1290457745312.jpg.html

turn out to make instructive mathematical insight[3]. What will interest us is that many of the points discussed above are not respected:

(1) Many steps are ambiguous and unclear: What exactly is done when "removing corners"? There are several ways to do it (e.g. one should specify the size of a corner): how should it be done? What exactly is meant by "remove more corners"? Most importantly (and this is where the argument goes wrong), what does it mean to "repeat to infinity"?
(2) Steps are only briefly justified by a picture. Pictures are very useful in mathematics as an additional explanatory device but can often be misleading (for example[4], it is possible to cut a ball into a few pieces, move these pieces around, and reassemble those pieces into two balls of the same volume as the earlier one). In general, a picture can never by itself justify a step. Here, the fact that the square with removed corners becomes a circle as we "repeat to infinity" is only justified with a picture of a circle.
(3) The hard step of the proof (the "repeat to infinity") is not emphasized at all and is written off as just some ordinary easy inference.

After making all those observations, it is no surprise that the proof turns out to be dead wrong. On the other hand, this proof also has some positive aspects: it is fun and very easy to read (since written in plain English, with additional pictures to illustrate) and has educational value!

We now look at a very different style of argument. We say a number x is *non-negative* if $x \geq 0$.

Theorem 2.3. For all non-negative real numbers a and b:

$$a^2 + b^2 \leq (a+b)^2$$

"Proof" 1.

$$\begin{aligned} a^2 + b^2 &\leq (a+b)^2 \\ a^2 + b^2 &\leq a^2 + 2ab + b^2 \\ 0 &\leq 2ab \end{aligned}$$

[3]Although this is beyond the scope of this course, this is also the case here: it turns out what makes the argument fail is that one cannot always invert the order of taking a limit and integrating.

[4]This is called the Banach-Tarski paradox, but is unfortunately beyond the scope of this course.

True because the product of two non-negative numbers is non-negative. □

First observe that in this case the result and its proof are clearly separated. The result is stated first (we will always call a true statement that we intend to prove a *theorem*[5]), followed by its proof. This is a good idea, as it helps the reader to see immediately what is being proven (as is traditional in mathematical writings, the end of the proof is marked by a box). In addition the argument consists of formal manipulations of equations, so one could hope it will make for a clear, unambiguous proof. There are however several issues: for one thing, one would have liked to see a plain English explanation of what exactly the argument is: as it turns out, each manipulation is correct, but how are they justified? Importantly, the first step is not at all justified, but is exactly what we want to prove! Thus a high level view of the "proof" is that we first assume what we want to prove, obtain a true conclusion, and therefore conclude the original assumption is correct. We will see that this is not logically valid, as it constitutes *circular reasoning* (for example, assume $0 = 1$ is true, multiply both sides by 0, get $0 = 0$, which is true. This does not justify $0 = 1$).

However, *in this particular case* one can revert all steps and obtain the correct conclusion. Thus a better proof is:

Proof 2. Since the product of non-negative numbers is non-negative,

$$0 \leq 2ab$$

Adding $a^2 + b^2$ to both sides, one gets:

$$a^2 + b^2 \leq a^2 + 2ab + b^2$$

So factoring the right hand side:

$$a^2 + b^2 \leq (a + b)^2$$

which is the desired inequality. □

It is of course more likely one would come up with an argument like "Proof" 1 first (keeping in mind that the steps can be reversed), but presented as such "Proof" 1 is incorrect and one must make sure to either mention that (and justify why) the argument is reversible, or write up a proof going in the right direction in the first place.

[5]Mathematicians usually make a distinction between theorems, lemmas and propositions depending on the importance of the result, but we will not adopt this approach

There are two different processes at work here: One is the process of *solving* the problem: coming up with all the ideas in the proof. The other is the process of *writing up* the proof itself. It is important that these two be separated: you are allowed to think about a problem in any way you like, but a proof has to satisfy stringent requirements and so must be written up with care.

Notice also that our proof takes several facts as a given. For one thing, the reader is expected to know what real numbers are, what sums and products are, and how they interact with the ordering (e.g. the fact that a product of non-negative numbers is non-negative). We state these facts precisely in the next section and prove a few useful results about the real numbers. This will provide us with examples for a more careful study of the basic logical reasoning involved in proofs (Section 4).

3. Numbers and inequalities

Tentative lecturing plan: The axiom of the real numbers, the definition of subtraction and division, the basic facts that follow, and the definition of the square should be covered in lecture 2. The definition of the square root, absolute value, the triangle and AGM inequalities should be covered in lecture 3.

3.1. **The real numbers.** You are probably already familiar with the real numbers. They are a basic object of study in calculus. Examples of real numbers include $0, 1, -1, \frac{1}{2}, \pi, e, \sqrt{2}$; Operations on real numbers include addition, multiplication, subtraction, division, square root, exponentiation, limits, etc.

It is unfortunately very tricky to correctly *define* what a real number is. You may be used to thinking of a real number as an integer followed by a dot and a (possibly infinite) sequence of digits. For example, $\pi = 3.14159265\ldots$. This "definition" turns out to have several issues. For one thing, such a sequence of digit is *not* unique (for example there is the infamous fact that $1 = 0.999999999\ldots$). More importantly, this definition does not tell us much about what a real number "really is": it just gives us a way to represent one, but there are many other choices (for example, one could use base 5 instead of base 10, or one could write $1/3$ instead of $0.3333333\ldots$) and it seems that an infinite sequence of digits is not particularly convenient to work with.

In this course, we will not discuss what real numbers really are, but will instead adopt an *axiomatic approach*: as discussed above, no matter what they are, we all know they must satisfy some properties (for example, $x < x + 1$ for any real number x). We will give a list of

such properties, and start from them (and only from them) to derive other nontrivial facts.

Axiom 3.1 (Axioms of real numbers)**.** [6] The real numbers are objects satisfying the following properties:

- (R_0) Among the reals, there are two distinguished elements, 0 and 1, with $0 \neq 1$. 0 and 1 have some special properties discussed below.
- (R_1) Binary operations $+$ and $\cdot$ are defined on the reals (they take two reals as input and produce one real as output).
- (R_2) Between any two reals x and y, one can ask whether $x < y$.
- Addition ($+$) satisfies the following properties: For all real numbers x, y, z:
  - (A_0) Associativity: $(x + y) + z = x + (y + z)$.
  - (A_1) Commutativity: $x + y = y + x$.
  - (A_2) Zero is the additive identity: $x + 0 = x$.
  - (A_3) Existence of inverse: There is always a unique[7] real number w such that $x + w = 0$.
- Multiplication ($\cdot$) satisfies the following properties: For all real numbers x, y, z:
  - (M_0) Associativity: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
  - (M_1) Commutativity: $x \cdot y = y \cdot x$.
  - (M_2) One is the multiplicative identity: $x \cdot 1 = x$.
  - (M_3) Existence of inverse: If $x \neq 0$, there is a unique real number w such that $x \cdot w = 1$.
- Multiplication and addition interact as follows: For all real numbers x, y, z:
  - (D_0) Distributive law: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.
- The ordering ($<$) satisfies the following properties: For all real numbers x, y, z:
  - (O_0) Trichotomy: exactly one of the following is true: $0 < x$, $x = 0$, or $x < 0$.
  - (O_1) Closure under addition: If $0 < x$ and $0 < y$, then $0 < x + y$.
  - (O_2) Closure under multiplication: If $0 < x$ and $0 < y$, then $0 < x \cdot y$.
  - (O_3) If $x < y$, then $x + z < y + z$.

[6] In this course, an "Axiom" is a basic principle that we assume as a given. A "Fact" is a result which follows from the axioms but will not be proved: you can take it as a given.

[7] In fact, uniqueness follows from the other properties (exercise).

- (C_0) The completeness axiom (*will not be discussed in this course*): If F is a non-empty collection of real numbers and there is a real number x such that for all y in F, $y < x$, *then* one can choose x with the additional property that for any $x' < x$ there is y in F with $x' < y$.

This is a very long list and you are not expected to learn all the properties by heart, nor remember their names. The completeness axiom is especially tricky and you will not be required to know anything about it. It turns out that those axioms *characterize* the reals: in a very precise sense only the real numbers satisfy those axioms. In fact, all true results about the reals can be proven using only these properties.

Before discussing the properties further, we introduce some notation:

Notation 3.2. When brackets are not present, multiplication should be done first, i.e. for x, y real numbers, $x \cdot y + x$ means $(x \cdot y) + x$, and *not* $x \cdot (y + x)$. We often write xy instead of $x \cdot y$. By associativity, the order of summation does not matter, so we write $x+y+z$ for $(x+y)+z$ (which is the same thing as $x + (y + z)$). Similarly for multiplication[8].

We write $y > x$ to mean $x < y$. We write $x \leq y$ to mean that $x < y$ or $x = y$. $x \geq y$ means $y \leq x$. We say x is *positive* if $0 < x$, *negative* if $x < 0$, *non-negative* if $0 \leq x$. When we want to emphasize that x is not zero, we may say "strictly positive" or "strictly negative".

Notice that it is necessary to explicitly define relations such as $>$ since all our axioms talk about is $<$. We can similarly define subtraction and division:

Definition 3.3. For x a real number, we define the *negative* of x to be the *unique* real number w such that $x + w = 0$ (this is guaranteed to exist by the axiom of existence of additive inverse). We write $-x$ for the negative of x. Similarly, define the *reciprocal* of a nonzero x to be the *unique* w such that $xw = 1$. We write x^{-1} for the reciprocal of x.

For real numbers x, y, we define $x - y$ to mean $x + (-y)$. Similarly, for y nonzero, we define x/y (also written $\frac{x}{y}$) to mean $x \cdot y^{-1}$.

Definition 3.4. The number 2 is defined to be $1 + 1$. Similarly, $3 = 1 + 1 + 1$, $4 = 1 + 1 + 1 + 1$, etc. The *natural numbers* are $0, 1, 2, 3, \ldots$ (a more precise definition will be given later in the course).

The *integers* consist of the natural numbers and their negative. The *rational numbers* consist of all numbers of the form n/m where n, m are integers and m is not zero.

[8]Associativity is used so often that we will never mention we are using it. Note that not all operations are associative. For example, subtraction is not: $(0-1)-1 = -2$ is different from $0 - (1 - 1) = 0$

Remark 3.5. Even though it has been thousands of years since the number 0 was introduced, some people are still debating whether the "right" definition of the natural numbers should contain zero. Depending on the kind of mathematics one is doing, it may or may not be convenient to have it included, and your experience with other courses may vary. From a foundational point of view, there are several good arguments for zero to be a natural number. The computer scientist Edsger Dijkstra has also given several other simple reasons [Dij]. Thus in this course, we will assume that 0 is a natural number.

You may take the following facts for granted. We will prove them once we have the tools to state a more formal definition of the natural numbers.

Fact 3.6.

(1) For all integers m and n, $m + n$ and $m \cdot n$ are integers.
(2) For all natural numbers m and n, $m + n$ and $m \cdot n$ are natural numbers.

From the axioms and the definitions of subtraction and division, we can go on to prove many more elementary properties. The arguments are usually quite boring (you will be asked to do a few of them in your homework). We list here all the elementary facts we will need (you can use them freely).

Fact 3.7 (Properties of addition and multiplication)**.** For all real numbers x, y, z, w:

- (F_0): $x \cdot 0 = 0$.
- (F_1): $-(xy) = (-x)y$.
- (F_2): $-x = (-1)x$.
- (F_3): $(-x)(-y) = xy$.
- (F_4): If $xy = 0$, then $x = 0$ or $y = 0$ (or both).
- (F_5): $(x + y)(z + w) = xz + xw + yz + yw$.

Fact 3.8 (Properties of the ordering)**.** For all real numbers x, y, z, w:

- (F_6): Totality: Exactly one of $x < y$, $x = y$, $y < x$ always holds. Exactly one of $x \leq y$ or $y < x$ always holds.
- (F_7): Reflexivity: $x \leq x$.
- (F_8): Antisymmetry: If $x \leq y$ and $y \leq x$, then $x = y$.
- (F_9): Transitivity: If $x \leq y$ and $y \leq z$, then $x \leq z$. Similarly if $\leq$ is replaced by $<$.
- Interaction with addition and multiplication:
  - (F_{10}): $0 < 1$.

- (F_{11}): If $x \leq y$ and $z \leq w$, then $x + z \leq y + w$. Similarly if $\leq$ is replaced by $<$.
- (F_{12}): If $x \leq y$, then $-y \leq -x$. Similarly if $\leq$ is replaced by $<$.
- (F_{13}): If $x \leq y$ and $0 \leq z$, then $xz \leq yz$.
- (F_{14}): If $0 \leq x$ and $0 \leq y$, then $0 \leq xy$. Similarly if $\leq$ is replaced by $<$.
- (F_{15}): $0 \leq x \cdot x$, and if $0 < x$ then $0 < x \cdot x$.
- (F_{16}): If $0 < x$, then $0 < x^{-1}$.
- (F_{17}): If $0 < x < y$, then $0 < y^{-1} < x^{-1}$.

Remark 3.9. Given real numbers x, y, z, if $x \leq y$ and z is arbitrary, then we *cannot conclude* that $xz \leq yz$: the hypothesis that $0 \leq z$ is needed. To see this, we give a *counterexample*: Take $x = 1$, $y = 2$, and $z = -1$. Then $x < y$ (exercise) but $zy < zx$ (by (F_{12}) and (F_2)).

We will use Fact 3.1 and Fact 3.7 without explicitly mentioning them each time.

3.2. **Squares, roots, and absolute value.**

Notation 3.10. For x a real number, we write x^2 for $x \cdot x$.

Theorem 3.11. For all real numbers x and y:

- $(x + y)^2 = x^2 + 2xy + y^2$.
- $(x - y)^2 = x^2 - 2xy + y^2$.
- $(x + y)(x - y) = x^2 - y^2$.

Proof. We use property (F_5) of Fact 3.7 and do the algebraic manipulations you should all be familiar with. For example:

$$\begin{aligned}(x+y)^2 &= (x+y)\cdot(x+y)\\ &= x^2 + xy + yx + y^2\\ &= x^2 + xy + xy + y^2\\ &= x^2 + 1\cdot xy + 1\cdot xy + y^2\\ &= x^2 + (1+1)xy + y^2\\ &= x^2 + 2xy + y^2\end{aligned}$$

The other proofs are similar. □

Remark 3.12. We will often call the process of going from a sum (as in $x^2+2xy+y^2$) to a product (as in $(x+y)^2$) *factoring*. We refer to the inverse operation (going from the product to the sum) as *expanding*.

Definition 3.13. A real number x is said to be a *square root* of a real number y if x is non-negative and $x^2 = y$.

By property (F_{15}) from Fact 3.7, x^2 is always non-negative, so *only non-negative real numbers have a real square root.* Moreover, the square root is unique:

Theorem 3.14 (Uniqueness of the square root)**.** Given x, y non-negative real numbers, assume $x^2 = y^2$. Then $x = y$.

Proof. Subtracting y^2 from both sides, we have that $x^2 - y^2 = 0$. Factoring, $(x - y)(x + y) = 0$. Thus (by (F_4)) either $x - y = 0$ (and so $x = y$) or $x + y = 0$ (and so $x = -y$). In the first case, we are done. In the second case, since $0 \leq x$, we must have $0 \leq -y$, so taking the negation on both sides and reversing the inequality (see (F_{12})), $y \leq 0$, and so by antisymmetry (F_8), $y = 0$. Therefore $x = -y = (-1)y = 0 = y$, as desired. □

Remark 3.15. This is an example of what is called *a proof by cases*: We show that one of two cases must happen, and show that from each one we can prove the result, so the result must be true.

We will not discuss the proof here (it uses the completeness axiom), but square roots exist:

Fact 3.16. Every non-negative real number has a square root.

Notation 3.17. For x a non-negative real number, we write $\sqrt{x}$ for the unique square root of x.

Example 3.18. We have that $\sqrt{4} = 2$, $\sqrt{1} = 1$, $\sqrt{0} = 0$. We will see later that $\sqrt{2}$ is a real number that is *not* rational.

Warning. Assume that x, y are real numbers and $x^2 = y$. Do we have $x = \sqrt{y}$? *No*, because we do *not* know that x is non-negative. Indeed, it turns out that $-\sqrt{y}$ is also a possible solution, which will be different from $\sqrt{y}$ if $y > 0$. Using uniqueness of the square root, it is not hard to see that these are the only possible solutions.

How do square roots play with the ordering? It turns out taking a square root preserves the ordering.

Theorem 3.19. For x, y real numbers, if $0 \leq x \leq y$, then $x^2 \leq xy \leq y^2$ and $\sqrt{x} \leq \sqrt{y}$.

Proof. Multiplying the first inequality by x (remembering that x is non-negative), we obtain $x^2 \leq xy$. Similarly, multiplying the first inequality by y, we obtain $xy \leq y^2$. Thus we obtain $x^2 \leq xy \leq y^2$.

To see $\sqrt{x} \leq \sqrt{y}$, we assume it is not true. Then we must have $x \neq y$ and $\sqrt{y} < \sqrt{x}$. By definition of the square root, $\sqrt{y}$, $\sqrt{x}$ are both non-negative, thus we can apply the fact we just proved (x standing for $\sqrt{y}$, y standing for $\sqrt{x}$) to get that $(\sqrt{y})^2 \leq (\sqrt{x})^2$, so $y \leq x$. Because $y \neq x$, $y < x$, a contradiction to the assumption. □

Remark 3.20. This is an example of a *proof by contradiction*: The result we want can be either true or false. We assume it is false and derive something ridiculously wrong, so the result must have been true in the first place.

Finally, we observe that taking square root and squares preserve products:

Theorem 3.21. For all real numbers x and y:

- $(xy)^2 = x^2y^2$.
- If x and y are non-negative, $\sqrt{xy} = \sqrt{x}\sqrt{y}$.

Proof. Exercise. □

Definition 3.22. The *absolute value* $|x|$ of a real number x is defined by:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

Theorem 3.23 (Elementary properties of the absolute value)**.** For all real numbers x and y:

(1) $x^2 = |x|^2$.
(2) $|x| = \sqrt{x^2}$.
(3) $x \leq |x|$.
(4) $|xy| = |x||y|$.

Proof. Exercise. □

3.3. **Inequalities.** Sometimes, it is very hard to know what a given quantity is *exactly* equal to, but it is possible to *estimate it*, namely give a lower (or upper) bound for it. This is what we will now investigate. We start with perhaps the most important inequality involving the real numbers, which allows us to estimate the absolute value of a sum in terms of the sum of the absolute values.

Theorem 3.24 (The triangle inequality)**.** For all real numbers x, y, $|x + y| \leq |x| + |y|$.

Proof. First observe that $2xy \leq 2|x||y|$ (to see this, first use Theorem 3.23.(3) to obtain $2xy \leq |2xy|$, and then use Theorem 3.23.(4) to see $|2xy| = 2|x||y|$). Adding $x^2 + y^2$ to both sides and using that $x^2 = |x|^2$ and $y^2 = |y|^2$, one obtains $x^2+2xy+y^2 \leq |x|^2+2|x||y|+|y|^2$. Factoring, $(x + y)^2 \leq (|x| + |y|)^2$. Since $(x + y)^2 = |x + y|^2$, we can take the square roots on both sides of the inequality and obtain the result from Theorem 3.19. □

Remark 3.25. It is often valuable to try to understand when an inequality is strict (meaning that $\leq$ can be replaced by $<$) and when it is not. In case of the triangle inequality, we can give examples for both cases: If $x = y = 1$, equality holds, while if $x = 1$ and $y = -1$, the inequality is strict. Can you come up with a condition on x and y characterizing when the inequality is strict?

For more practice, we prove the following important inequality:

Theorem 3.26 (The arithmetic mean, geometric mean (AGM) inequality)**.** For all non-negative real numbers x, y, $\sqrt{xy} \leq \frac{x+y}{2}$.

Proof. Note first that since x and y are non-negative, xy is non-negative (by (F_{14})), so it makes sense to talk about $\sqrt{xy}$.

We start the proof by observing that $0 \leq (x-y)^2$ (because squares are always non-negative (F_{15})). Expanding and adding $2xy$ on both sides, we obtain $2xy \leq x^2+y^2$. Adding $2xy$ again and factoring the right hand side, we get $4xy \leq (x + y)^2$. By Theorem 3.19, $\sqrt{4xy} \leq \sqrt{(x + y)^2}$. Using Theorem 3.21, we can expand the left hand side to $2\sqrt{xy}$. Using Theorem 3.23, $\sqrt{(x + y)^2} = |x + y| = x + y$ (since both x and y are non-negative and a sum of non-negative numbers is non-negative by (F_{11})). Thus we obtain $2\sqrt{xy} \leq x + y$, so (using (F_{16}) to see that $\frac{1}{2}$ is positive and (F_{13}) to multiply both sides by $\frac{1}{2}$) $\sqrt{xy} \leq \frac{x+y}{2}$, as desired. □

Remark 3.27. In the AGM inequality, equality holds precisely when $x = y$: First, it is not difficult to check that equality holds if $x = y$. Now if $x \neq y$, then $0 < (x - y)^2$, and one can repeat the proof with $\leq$ replaced by $<$, so the inequality ends up being strict.

4. Basic logic

Lecture 4 will cover the basic logical operators, Lecture 5 will cover quantifiers (tentative)

We now start our study of the *elementary logic* inherent in all mathematical reasonings (including the reasonings done in the past section).

Believe it or not, we have already been doing quite a bit of logic in the past section: For example, we used words such as "for all", "for any", "exists", "assume", "if", "then", "and", "or", "therefore", "thus", etc (some are synonyms). In mathematics, those words have a very precise meaning, sometimes different from their colloquial use in English. Since proofs must be unambiguous, it is important that everybody agrees on what those words *exactly* mean. This will allow us to discuss questions that are very foreign to everyday English. For example, we will see what exactly should be proven to show that the statement "For any non-negative real number x, if $x \neq 2$, then either $0 = 1$ or $x \neq 3$" is false.

We start with the basic concept of a *proposition*. A proposition is an unambiguous mathematical statement that is either true or false[9]. Examples include:

- Every real number has a real square root.
- For all real numbers x and y, $|x + y| \leq |x| + |y|$.
- Every even natural number strictly larger than 2 is the sum of two primes.
- $2 + 3 = 5$.
- $2 + 2 = 7$.

The first and last propositions are false (why?), but nevertheless they have a clear mathematical meaning. The third example[10] (do not worry if you do not remember what an even number or a prime is) is also a proposition, but interestingly, mathematicians do not know (as of May 2014) whether it is true or false. Most *believe* it is true, but nobody knows a proof. Such propositions are called *conjectures*. We will see that we can reason with propositions, even if we do not know whether they are true or false.

On the other hand, the following are not propositions:

- Mathematics is boring.
- 42.

The first one has no precise mathematical meaning, while the second one has no truth value (it is not saying something which is either true or false).

[9]You may object (and you would be right) that this is not a good definition, since we have left undefined what words like "mathematical statement", "true", and "false" mean. Making all of this completely precise would force us to introduce programming language-like formalisms that, while essential to a deeper understanding of mathematical reasonning, are dry and not too relevant in everyday mathematical practice. We will not go down that road here.

[10]Which goes by the name of Goldbach's conjecture.

4.1. **Logical operators.** We can combine propositions using *logical operators* such as *and* or *or*. For example, "$2 + 3 = 5$ or $2 + 2 = 7$" is a proposition. Is it true or false? It is true: in mathematics, the "or" (also called the *disjunction*) of two propositions is true when *at least* one of them is true (so "or" is inclusive: "$2 + 3 = 5$ or $3 + 2 = 5$" is true). Notice that this does not always match English usage. For example when in a restaurant you are told that your side can be either French fries or cole slaw, this means you cannot choose both (unless you pay extra). On the other hand, if while on a beach you are told that you should protect yourself from the sun using a cap or a T-shirt, this means it is also fine if you use both.

Closer to English usage, the "and" (also called the *conjunction*) of two propositions is true when *both* propositions are true. Thus "$2+3 = 5$ and $2 + 2 = 7$" is false, but "$2 + 3 = 5$ and $3 + 2 = 5$" is true.

When considering compound propositions with many ands and ors, using English becomes annoying, so we introduce a formal "algebra" of propositions. We specify that the simplest propositions will be T (which simply abbreviates true and is always true) and F (which is always false).

For p and q propositions, we introduce symbols to stand for "or" and "and": we will write $p \vee q$ for p or q, and $p \wedge q$ for p and q. We *define* these operators using a *truth table*. A truth table specifies exactly how an operator behaves by simply listing all possible truth values for p and q. Here is the truth table of $\vee$ and $\wedge$:

p	q	$p \vee q$	$p \wedge q$
F	F	F	F
F	T	T	F
T	F	T	F
T	T	T	T

For example, the first line tells us that if both p and q are false, then $p \vee q$ and $p \wedge q$ are also false. Using truth tables, we can reason about propositions without worrying about the ambiguities of the English language. Let's now introduce more operators!

A seemingly simple operator is the *negation*: The *negation* of a proposition p, written $\neg p$ and read "not p", is false if the proposition is true, and true if it is false. Using a truth table, this translates to:

p	$\neg p$
F	T
T	F

Since the "and" of two propositions is also a proposition, we are allowed to take its negation. To avoid ambiguities, we use brackets to say which operation is to be done first. $\neg(p \wedge q)$ takes the negation of $p \wedge q$, while $(\neg p) \wedge q$ first takes the negation of p, and then "and"s this with q. By convention, negations are taken first, so $\neg p \wedge q$ will say the same thing as $(\neg p) \wedge q$.

Is there a simple way of expressing the negation of $p \wedge q$? Let's see what this would say in plain English: if I know that it is false that both p and q hold, what do I know about p and q? Well, *at least* one of them must be false. Said symbolically, $\neg p \vee \neg q$. Since it is tricky to conduct those reasonnings in plain English, you should *not* consider the previous sentences as a proof, only as an indication of what you are looking for. To make our argument precise, let's use a truth table:

p	q	$\neg p$	$\neg q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$
F	F	T	T	F	T	T
F	T	T	F	F	T	T
T	F	F	T	F	T	T
T	T	F	F	T	F	F

We see that indeed $\neg(p \wedge q)$ and $\neg p \vee \neg q$ behave in exactly the same way. We say that they are *logically equivalent* (or just equivalent) and write $\neg(p \wedge q) \equiv \neg p \vee \neg q$. This result has a name:

Theorem 4.1 (De Morgan's laws for logical operators)**.** For all propositions p and q:

- $\neg(p \wedge q) \equiv \neg p \vee \neg q$.
- $\neg(p \vee q) \equiv \neg p \wedge \neg q$.

Proof. The first result has just been proven, and the proof of the second is similarly done using a truth table (exercise). □

We now introduce an important and often misunderstood operator: implication.

Definition 4.2. For propositions p and q, the operator $p \to q$ (read "p implies q", or "if p, then q") is *defined* by the following truth table:

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

Notice that if p is false, then $p \to q$ is true *regardless of* q (using our notation, $F \to q \equiv T$). For example, both $(0 = 1) \to (1 = 1)$ and

$(0 = 1) \to (1 \neq 1)$ are true propositions. This may be best understood by an example: Consider the statement "If it is raining, then the road is wet". The only way this statement could be *false*, is if there had been a day when it was raining, yet the road wasn't wet. The statement does not tell us anything about days when it is not raining: in that case, the road may or may not be wet (maybe the road is near the sea and waves can reach it, or maybe it's just some road in the desert where it never rains).

Concretely, this means that to *prove* that a statement of the form $p \to q$ is true, it suffices to *assume* p is true (since if p is false, the statement holds regardless of q), and show that q must also be true.

We can express $p \to q$ using the operators previously defined:

Theorem 4.3. For all propositions p and q, $p \to q \equiv \neg p \vee q$.

Proof. Exercise. □

Note that even if $p \to q$ is true, this does *not* necessarily mean that $q \to p$ holds. Using the previous example, even if we know that the road gets wet whenever it is raining, we cannot conclude that it is raining from the fact the road is wet (maybe somebody just poured some water on it). This is a *very* common source of errors. Another operator expresses this case:

Definition 4.4. For propositions p and q, the operator $p \leftrightarrow q$ (read "p if and only if q", or "p and q are logically equivalent") is *defined* by the following truth table:

p	q	$p \leftrightarrow q$
F	F	T
F	T	F
T	F	F
T	T	T

Theorem 4.5. $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$.

Proof. Exercise. □

4.2. **Quantifiers.** A proposition such as "For any real number x, $0 \leq x^2$" can be seen as a simple "propositional function", $0 \leq x^2$, together with a *universal quantifier* "For any real number" telling us that this holds regardless of the exact value of x. Notice that this is more complicated than simply saying something like "$0 \leq 1^2$ and $0 \leq 2^2$". We now enlarge our "algebra of propositions" with such quantifiers.

First, we introduce the notion of a *propositional function*. A *propositional function* is a statement with variables that become a proposition

once the variables are assigned values. For example, $0 \leq x^2$ is not a proposition since it has no meaning if we do not specify x, but it become a proposition once x is specified. We could of course have more than one variable, as in $x = \sqrt{y}$. The truth value of the propositional function could depend on the value of the variables. For example, $x = \sqrt{y}$ is true if $x = y = 0$, but false if $x = -1$ and $y = 0$. Note that it is *implicit* that the variables always take their values in a particular *domain of discourse* (here the real numbers). It is always a good idea to state this domain of discourse explicitly.

Given a propositional function $p(x)$ with variable x, we would like to turn it into a proposition. We have already seen one way to do it: plug in a particular value for x. Another way is to qualify it with a *quantifier*. We will consider two of them here: "for all" and "there exists".

Definition 4.6. Assume $p(x)$ is a propositional function with variable x.

We define the proposition $\forall x\ p(x)$ (said "For all x, $p(x)$", or "For any x, $p(x)$") to be true precisely if $p(x)$ is true for *any* value of the variable x in the domain of discourse.

We define the proposition $\exists x\ p(x)$ (said "There exists x such that $p(x)$", or "There is x such that $p(x)$") to be true precisely if $p(x)$ is true for *at least one* value of x in the domain of discourse.

Example 4.7.

- Formalizing the example above, we get $\forall x\ 0 \leq x^2$, where the domain of discourse is the real numbers.
- We can formalize the statement "For any non-negative real number x, if $x \neq 2$, then either $0 = 1$ or $x \neq 3$" by $\forall x\,(x \neq 2 \to (0 = 1 \vee x \neq 3))$, where the domain of discourse is the non-negative real numbers. Alternatively, we could set the domain of discourse to be all the real numbers, and formalize the statement by:

$$\forall x\,(x \geq 0 \to (x \neq 2 \to (0 = 1 \vee x \neq 3)))$$

- We can formalize the statement "Every real number has a real square root" by $\forall x \exists y\ (y^2 = x \wedge y \geq 0)$. The domain of discourse is again the real numbers.
- The statement of the triangle inequality can be written as $\forall x \forall y\ |x+y| \leq |x| + |y|$.
- The statement p that every even natural number strictly larger than 2 is the sum of two primes can be said in many different ways. Let Prime(x) stand for the statement "x is a prime

number, and Even(x) stand for the statement "x is an even number". Then p can be written:

$$\forall x \left((\text{Even}(x) \wedge x > 2) \rightarrow (\exists y \exists z \ \text{Prime}(y) \wedge \text{Prime}(z) \wedge x = y + z)\right)$$

Where the domain of discourse is the natural numbers.

Several remarks are in order. First, formalizing statements in this way can make them hard to read, so it is best to use this kind of notation sparingly and prefer plain English when there is no ambiguity. On the other hand, once formalized, we will see it is easy to reason about the statement itself (e.g. to take its negation, or to see what exactly one will have to do to prove the statement). Translating from English could be a bit tricky, since there are many synonyms to express the same thing. For example, "Assume x is a real number, then $0 \leq x^2$", "Let x be a real number, then $0 \leq x^2$", "For any real number x, $0 \leq x^2$" are all saying the same thing.

Notice also that the truth of a proposition could depend on the domain of discourse. For example,

$\forall x \exists y \ y^2 = x$ is false if the domain of discourse is the real numbers (why?) but it is true if the domain of discourse is the *non-negative* real numbers.

We now turn to the interplay between quantifiers and negations: Assume $p(x)$ is a propositional function with variable x. Is there a simple way to write $\neg \forall x \ p(x)$? Unfortunately, we cannot use truth tables to figure it out anymore, but we can still think about what the question means in plain English: what does it mean for example to say that not all sheep are black. Well, there must exist a *counter-example*: a sheep that is not black. Thus $\neg \forall x \ p(x)$ is *logically equivalent* (i.e. $(\neg \forall x \ p(x)) \leftrightarrow (\exists x \ \neg p(x))$ is always true) to $\exists x \ \neg p(x)$. Similarly, if it is false that there exists a black sheep, this means no sheep is black, or in other words, all sheep are non-black. In symbols, $\neg \exists x \ p(x) \equiv \forall x \ \neg p(x)$. We will unfortunately not be able to *prove* these laws, since to avoid spending too much time on boring formalisms, we have avoided defining words such as "propositions" too precisely. We will see them as basic laws of reasoning that should be taken as granted. We state them again for reference:

Axiom 4.8 (De Morgan's laws for quantifiers)**.** For any propositional function $p(x)$:

- $\neg \forall x \ p(x) \equiv \exists x \ \neg p(x)$.
- $\neg \exists x \ p(x) \equiv \forall x \ \neg p(x)$.

To see the analogy with De Morgan's laws for logical operators, you should think of $\forall x$ as a possibly infinite "and" over all the elements of the domain of discourse, and $\exists x$ as a similar possibly infinite "or".

Concretely, this shows us that to *disprove* a statement of the form "For all x, $p(x)$", it is enough to find one x such that $\neg p(x)$ (a *counterexample*). Recall that we had already used this reasoning unconsciously before.

Example 4.9. The negation of the proposition "Every real number has a square root" is:

$$\begin{aligned}\neg\forall x\exists y\ y^2 = x &\equiv \exists x\neg\exists y\ (y^2 = x \wedge y \geq 0)\\ &\equiv \exists x\forall y\ \neg(y^2 = x \wedge y \geq 0)\end{aligned}$$

This tells us that to prove that "Every real number has a square root" is false, it is enough to prove that there exists a real number x such that for every real number y, y is not the square root of x, or in other words, there exists a real number that is not the square of any other (non-negative) real number (This is true, since one can take $x = -1$).

We close with an important warning: *the order of quantifiers matters*: For $p(x, y)$ a propositional function, the statements $\forall x\exists y\ p(x, y)$ and $\exists y\forall x\ p(x, y)$ are *not* logically equivalent. Let's think about an everyday example: assume $p(h, k)$ is the statement "k is a key that unlocks the door of house h". The statement "$\forall h\exists k\ p(h, k)$" says that for any fixed house, there is a key that opens its door. This sounds reasonable. On the other hand, the statement "$\exists k\forall h\ p(h, k)$" says that there is a key that opens *every* house. In the first statement, each door might be opened by a different key, but the second statement tells us that *the same* key opens every door.

Example 4.10. Here is a more mathematical example: The statement "For every real number x, there is a real number y such that $x < y$" is true (why? If x is a real, then $y = x + 1$ does the job), but the statement "There exists a real number y such that for every real number x, $x < y$ is false (why? Given any real number y, $x = y + 1$ is such that $\neg(x < y)$).

We will see that it *is* always true that $(\exists y\forall x\ p(x, y)) \to (\forall x\exists y\ p(x, y))$. You may want to convince yourself of this fact before moving on.

5. Elementary proof techniques

Lecture 6 started here

Now that we have some understanding of mathematical statements, let's look at some of the most useful techniques to prove them.

Assume you are given a proposition p which you would like to prove is true (note that if instead you want to prove that it is *false*, then it is the same as proving that $\neg p$ is true, and we have seen some tools in the previous section to make $\neg p$ into a simpler equivalent proposition ("pushing the negation inside")). You should realize that there is no algorithm or clear method that always works. However, there are some logical steps that are useful to know about and show up over and over again when proving certain types of statements. This is what this section focusses on.

5.1. **Direct proof.** This is the simplest method and the one that you should try first. You are given p a proposition you would like to prove. Let's look at what form your proposition could have. First it could be that p is so simple you can determine its truth value right away, e.g. maybe it is T (or maybe you can see by truth table that it is logically equivalent to T), or maybe it is $0 \neq 1$ (which is true simply because it is an axiom), etc.

Most often however, your proposition is too complicated to just be an axiom, but instead will be a *compound* proposition, i.e. it will contain simpler propositions that are put together using and, or, implies, quantifiers, etc. We would like to reduce the problem of proving p to the problem of proving these simpler propositions. It turns out that for each logical operator, there is a clear direct method of doing so. Below, q and r are propositions.

- If p is $q \wedge r$, then it is enough to prove both q and r.
- If p is $q \vee r$, then it is enough to prove one of q or r.
- If p is $q \to r$, then it is enough to prove r *assuming* q, i.e. you can take q for granted in your proof of r. q is often called the *hypothesis*, and r the *conclusion* of the statement p.
- If p is $q \leftrightarrow r$, then it is enough (since they are equivalent by Theorem 4.5) to prove both $q \to r$ and $r \to q$. The statement $r \to q$ is called the *converse* of $q \to r$.

We can similarly give similar guidelines for quantifiers. Below, $q(x)$ is a propositional function.

- If p is $\exists x\ q(x)$, then it is enough to exhibit some element a in the domain of discourse such that $q(a)$ can be proven to be true.

- If p is $\forall x\ q(x)$, then it is enough to fix an arbitrary element a of your domain of discourse, and prove that $q(a)$ is true. This step is often expressed by a sentence such as "Let a be an arbitrary real number" (if the domain of discourse is the real numbers).

At an abstract level, proving a statement boils down to managing a list of known facts and axioms, and *using* them wisely to obtain the result. The facts we know can also be written as propositions, so let's see how we can use them. Assuming we already *know* that proposition p is true, we can similarly unpack p to make it more transparent. Below, q and r are propositions.

- If p is $q \wedge r$, then we know both q and r.
- If p is $q \vee r$, then we know that at least one of q or r is true.
- If p is $q \to r$, then whenever we also know that q holds, we know that r holds.
- If p is $q \leftrightarrow r$, then we know both that $q \to r$ and $r \to q$.

Let's finally look at what happens if p has quantifiers. Below, $q(x)$ is a propositional function.

- If p is $\forall x\ q(x)$, then for an *arbitrary* element a in the domain of discourse, $q(a)$ will be true.
- If p is $\exists x\ q(x)$, then we know that we can *pick* (or *fix*) an element a in the domain of discourse such that $q(a)$ is true.

You might think the above is just repeating redundant information about the meaning of propositions. Yet it turns out that those steps are used over and over again in almost any proofs, so it is useful to keep them in mind.

Remark 5.1 (From something false, anything follows)**.** The rules for dealing with known facts of the form $q \to r$ tells us something important about logical reasoning: Assume that q is a false proposition. From the definition of an implication, we know that $q \to r$, holds, *regardless of* r. Thus if we make a single "tiny" mistake in a mathematical proof and manage to show that q is true, we will be able to derive *any nonsense we like*[11]. This is why mathematicians put so much emphasis on correct proofs.

Let's try to use those principles on some example.

Theorem 5.2. For all propositional functions $p(x, y)$, $(\exists y \forall x\ p(x, y)) \to (\forall x \exists y\ p(x, y))$ is always true.

[11]The mathematician Bertrand Russel was once challenged by one of his student to prove from $0 = 1$ that he was the pope. Here is his proof: adding 1 to both sides of the equation, we get $1 = 1 + 1$. The pope and I, form 2 persons, but since $2 = 1$, we actually are only one person, therefore I am the pope.

Proof. We want to prove a statement of the form $q \to r$, where q is $\exists y \forall x\ p(x, y)$, and r is $\forall x \exists y\ p(x, y)$. Thus we assume q as a given, and want to prove r. r is of the form $\forall x\ s(x)$, where $s(x)$ is $\exists y\ p(x, y)$, thus we let a be an arbitrary element of the domain of discourse, and we want to show that $s(a)$ holds. This is an existential statement, so it is enough to exhibit a single b such that $p(a, b)$. For this, we use q: we know there exists a single y such that something depending on y holds. We *fix* such a y and take[12] $b := y$. q tells us that for an *arbitrary* x, $p(x, y)$, and so *in particular* if we take $x = a$, $p(a, b)$ holds. This is exactly what we wanted to show. □

For more practice, we continue playing with numbers.

Definition 5.3 (Even and odd integers)**.** An integer n is *even* if it can be written as $n = 2m$ for m an integer (or, in other words, if *there exists* an integer m such that $n = 2m$). n is *odd* if it can be written as $n = 2m + 1$ for m an integer.

Example 5.4. 0 is even, since $0 = 2 \cdot 0$. 2 is even, since $2 = 2 \cdot 1$. 1 is odd, since $1 = 2 \cdot 0 + 1$. We will see that a number is even exactly when it is not odd.

Theorem 5.5 (Sum of odds and evens)**.** Assume n and m are integers.

(1) n is even if and only if $-n$ is even. n is odd if and only if $-n$ is odd.
(2) If n and m are even, then $n + m$ is even.
(3) If n and m are odd, then $n + m$ is even.
(4) If n is odd and m is even, then $n + m$ is odd.
(5) If n is even, then nm is even.
(6) If n and m are odd, then nm is odd.

Proof.

(1) Assume first that n is even. Then $n = 2k$ for k an integer. Thus $-n = -2k = (-1)2k = 2(-1)k = 2(-k)$. Since k is an integer, $-k$ is also an integer (by definition of the integers), so $-n$ is even. For the converse, assume that $-n$ is even. Then by the first part $-(-n) = n$ is even, as desired. The proof of the second statement is similar (exercise).
(2) Assume that n and m are even. By definition, this means that $n = 2k$ for k an integer, and $m = 2k'$ for k' a possibly different

[12]We use $b := y$ instead of $b = y$ to emphasize that b is *defined* to be y (so $b = y$ is not a consequence of any previous fact). Mathematically, $b := y$ and $b = y$ mean the same thing.

integer. Thus we have that $n+m = 2k+2k' = 2(k+k')$. Since the sum of two integer is an integer (Fact 3.6), $n+m$ is even.

(3) Assume that n and m are odd. By definition, this means that $n = 2k+1$ for k an integer, and $m = 2k'+1$ for k' an integer. Thus we have that $n+m = 2k+1+2k'+1 = 2k+2k'+2 = 2(k+k'+1)$. Since the sum of two integer is an integer (Fact 3.6), $n+m$ is even.

(4) Assume that n is odd and m is even. By definition, this means that $n = 2k+1$ for k an integer, and $m = 2k'$ for k' an integer. Thus we have $n+m = 2k+1+2k' = 2(k+k')+1$. Since $k+k'$ is an integer, $n+m$ is odd.

(5) Exercise.

(6) Exercise.

□

As a particular case, we obtain that for any even integer n, n^2, $n+2$, and $n-2$ are even, and $n+1$ and $n-1$ are odd.

5.2. **Proof by contradiction.** We sometimes get "stuck" trying to apply the direct methods above. For example, assume we want to prove p which is of the form $\forall x\ q(x)$. Proving something holds for *every* element in the domain of discourse can be challenging, so sometimes it might be easier to derive a *contradiction* (i.e. a false proposition) from the negation of p. Formally, if we could show that $\neg p \to F$ is true, then looking at the truth table of the implication operator, this must mean that $\neg p$ is false, and hence that p is true. In symbol:

Theorem 5.6 (The principle of reasoning by contradiction)**.** For any proposition p, $(\neg p \to F) \to p$ is always true.

Proof. Exercise: use a truth table. □

The power of the method of proof by contradiction is that *when we want to prove p, we can assume $\neg p$ holds for free.* Let us look at an example:

Theorem 5.7. For any even integer n, n is not odd.

Proof. By definition $n = 2m$ for some integer m. We would like to show that n is not odd, i.e. it is false that there exists an integer k so that $n = 2k+1$, or equivalently, for any integer k, $n \neq 2k+1$. It is not so clear how to proceed, so we *assume for a contradiction* that the opposite is true, namely there exists an integer k so that $n = 2k+1$.

Then $2m = 2k+1$, so $2(m-k) = 1$, so $m-k = \frac{1}{2}$. Now recall that $0 < \frac{1}{2} < 1$ (why?), so $\frac{1}{2}$ cannot be an integer, but $m-k = m+(-k)$

is an integer by Fact 3.6. Thus we obtain the proposition "$m-k$ is an integer and $m-k$ is not an integer" which is a contradiction. Therefore it must be that n is not odd. □

Using a technique called *induction*, we will later prove:

Fact 5.8. Any integer is either even or odd (but not both by the previous theorem).

Here, lecture 6 ended and lecture 7 started.
From this, we can prove:

Theorem 5.9. For any integer n, n is even if and only if n^2 is even.

Proof. If n is even, then by Theorem 5.5 n^2 is even.

For the converse, assume n^2 is even, and suppose for a contradiction that n is not even. By the previous fact, it must be odd. But then n^2 is odd by Theorem 5.5. Since n cannot be both even and odd, this is a contradiction. □

Recall that a real number is rational if it can be written in the form n/m for n and m integers, m nonzero. A number which is not rational is called *irrational*. For the next example, we will also need (and this will also be proven later using induction):

Fact 5.10. Given a rational number r, there exists integers n and m with $r = n/m$, m nonzero, and at least one of n or m is odd.

Theorem 5.11. $\sqrt{2}$ is irrational.

Proof. We have to prove that there does *not* exist integers n, m with m nonzero and $\sqrt{2} = n/m$. It is unclear how to proceed, so we assume for a contradiction that this is false, i.e. $\sqrt{2}$ is rational. Use the previous fact to pick an integer n and a nonzero integer m such that at least one of them is odd and $\sqrt{2} = \frac{n}{m}$. Taking squares on both sides, $2 = \left(\frac{n}{m}\right)^2 = \frac{n^2}{m^2}$. Multiplying both sides by m^2, $2m^2 = n^2$. This shows that n^2 must be even, but then by Theorem 5.9, n is even. Thus $n = 2k$ for some integer k, and so $2m^2 = n^2 = 4k^2$. Hence $m^2 = 2k^2$ must be even, and hence m must be even. Since at least one of n or m must be odd, this is a contradiction. □

5.3. **Proof by cases.** Assume again that we want to prove the proposition p. We have already seen examples where we are stuck, but we would know what to do assuming some proposition q, and we would also know what to do assuming some proposition r. Assume further that we know that at least one of these always holds, i.e. $q \vee r \equiv T$. Then we are done proving p. In symbols:

Theorem 5.12 (The principle of reasoning by cases)**.** For all propositions p, q, r:
$((q \vee r) \wedge (q \to p) \wedge (r \to p)) \to p$ is always true.

Proof. Exercise: use a truth table. □

Very often, r will just be $\neg q$, and then $q \vee r$ is always true (why?). Let's look at an example. For this, we need to define the operation x^y for x a positive real number and y an arbitrary real number. This turns out to be very tricky, so we will just take the existence of this operation as a given:

Fact 5.13. There is an operation x^y for x a strictly positive real number and y a real number satisfying the following properties. For any strictly positive x, and real numbers y and z:

(1) $x^0 = 1$
(2) $x^1 = x$.
(3) $x^{y+z} = x^y \cdot x^z$.
(4) $(x^y)^z = x^{y \cdot z}$.

It turns out there are many such maps, and that to characterize the usual exponentiation, one needs to add the condition that for a fixed x the map $y \mapsto x^y$ is continuous. There is no need for you to worry about this detail here.

Theorem 5.14. There exists irrational numbers x and y such that x^y is rational.

Proof. We split our proof into two cases. Recall that $\sqrt{2}$ is irrational (Theorem 5.11).

Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational. Then we can take $x = y = \sqrt{2}$ which are irrational by the observation above.

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational. Then let $x := \sqrt{2}^{\sqrt{2}}$ and $y := \sqrt{2}$. x is irrational by assumption, y is irrational by the above, and

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = \sqrt{2}^{1+1} = \sqrt{2} \cdot \sqrt{2} = 2$$

which is rational.

Since for any proposition p, $p \vee \neg p$ is always true (exercise), we see that either case 1 or case 2 happens, so we are done. □

The downside of such a proof is that it is *nonconstructive*: It gives us no information as to *which case* is true. We know one of them must

be, but we do not know which one. It is a hard theorem of Kuzmin (beyond the scope of this course) that $\sqrt{2}^{\sqrt{2}}$ is actually irrational.

6. Introduction to sets

Previously, we "defined" the natural numbers to be 0, 1, 2, 3, ... What do these three dots actually mean? The intended meaning is that we keep adding 1 "forever", generating more and more natural numbers. This is of course a lousy explanation, but even if we accept it, how can we make this intended meaning precise? An alien ignorant of terrestrial mathematics might believe this means 0, 1, 2, 3, 2, 1, 0, ... How can we precisely tell such an alien what we mean?

At this point, the concept of a *set* becomes useful. The situation is somewhat analogous to the real numbers: you are probably already familiar with sets: examples include the empty set, the set of real numbers, the set of natural numbers, the set $\{0, 1, 4\}$, the set $\{a, b\}$, etc; Operations on sets include union, intersection, complementation, etc.

Similarly to the case of the real numbers, it is very tricky to *define* what a set is. Some textbooks define a set as a collection of objects. This is not very satisfying: isn't "collection" another word for "set"? Isn't this "definition" analogous to saying that a real number is a quantity denoting a magnitude?

Another issue is that the intuitive meaning of the term "collection" is not quite what is intended. For example, you will prove in your homework that there cannot be a set containing all sets.

In these notes, we will adopt an *axiomatic* approach: we assume that there are objects we call sets, and give a list of some of their properties.

Axiom 6.1 (First axioms of sets)**.** *Sets* are objects satisfying the following properties:

- ($\in$): Given an object a and a set A, we can ask whether a is in A (written $a \in A$). If $a \in A$, we say that a is an *element*, or a *member* of the set A.
- (E): Extensionality: A set is determined by its elements: for all sets A and B, if for any $a \in A$ we have $a \in B$, and for any $b \in B$ we have $b \in A$, then $A = B$.
- (S): Specification: Given a set A, and $p(x)$ a propositional function with variable x taking values in A, we can form the set B of elements of A satisfying p (written $B := \{a \in A \mid p(a)\}$. This is sometimes called the *set-builder notation*.). An object a will be in B exactly when it is in A *and* it satisfies $p(a)$.

- (P): Pairing: For any two (not necessarily distinct) objects a and b, we can form the set $A := \{a, b\}$. An object x will be in A exactly when $x = a$ or $x = b$.

We will introduce more axioms later, but some remarks are in order:

- We are effectively cheating, because we are not saying what an "object" is. You can just take it to mean "anything we will use sets with". For example, numbers are objects, but sets are also objects, so one can define a set containing other sets. We sometimes call such a set a *collection* of sets or a *family* of sets.
- Extensionality tells us in particular that *sets are unordered*: the sets $\{1, 2\}$ and $\{2, 1\}$ are the same. Later, we will define the notion of an *ordered pair*, and the ordered pair $(1, 2)$ will be different from the ordered pair $(2, 1)$.
- The pairing axiom tells us in particular that for any object a, we can form the set $\{a, a\}$ which by the extensionality axiom is the same as the set $\{a\}$ containing the single element a. We will see later how to form sets with more than two elements.
- In the axiom of specification, it is important that we start with a given set A, and then "refine" it to obtain a new set B. It is *not* possible to start with a propositional function $p(x)$ and form the set of all a such that $p(a)$. If it were possible, we could take $p(x)$ to be "x is a set", and form the set of all sets. You will see in your homework that it already follows from the axioms above such a set cannot exist.

From the axioms above, we can already form a special set that plays an important role:

Theorem 6.2 (Existence of the empty set)**.** There is a unique set that contains no elements. We write $\emptyset$ for this set.

Proof. By the axiom of pairing, we can form the set $A := \{1, 2\}$. By the axiom of specification, we can form $B := \{a \in A \mid F\}$ (recall that F denotes the proposition that is always false). By definition, B does not contain any element. B is unique with this property, since sets are determined by their elements. □

Remark 6.3. In mathematics, it often happens that we have to prove existence of a unique object satisfying some properties (like in the previous result). The proof of such a result usually has two parts: we prove the object exists, usually by constructing it, and then we prove it is unique by showing that any two objects with the required property must be the same.

We now define the important notion of being a subset:

Definition 6.4. A set A is a *subset* of a set B (written $A \subseteq B$) if for all $a \in A$, $a \in B$. We say A is a *proper subset* of B (written $A \subset B$) if $A \subseteq B$ but $A \neq B$. We write $A \supseteq B$ to mean $B \subseteq A$, and $A \supset B$ for $B \subset A$.

Remark 6.5. Some people write $A \subset B$ for $A \subseteq B$, while using $A \subsetneq B$ to emphasize that the inclusion is proper.

For example, $\emptyset \subseteq A$ for all sets A, and $\{1\} \subset \{1, 2\}$.

Directly from the axiom of extensionality, we obtain:

Theorem 6.6. Two sets A and B are equal if and only if $A \subseteq B$ and $B \subseteq A$.

Proof. If $A = B$, they have in particular the same elements, and so $A \subseteq B$ and $B \subseteq A$ follow. If $A \subseteq B$ and $B \subseteq A$, then the definition of the axiom of extensionality tells us that $A = B$. □

This tells us that in virtually all cases, *to prove that two sets are equal, we must show that each is a subset of the other.*

Just like for numbers and propositions, we would like to define some operation on sets. Here is one of the most important:

Definition 6.7. Given two sets A and B, the *intersection* of A and B (written $A \cap B$) is the set $\{a \in B \mid a \in A \text{ and } a \in B\}$.

More generally, let $\mathcal{F}$ be a nonempty family of sets. Pick some set $B \in \mathcal{F}$. The intersection of the family $\mathcal{F}$ (written $\bigcap_{A \in \mathcal{F}} A$) is the set

$$\{a \in B \mid a \in A \text{ for all } A \in \mathcal{F}\}$$

Thus the intersection of two sets is simply the set of all objects contained in both sets, and more generally, the intersection of a (possibly infinite) family of sets is the set of objects contained in all sets of the family. You should convince yourself that the definition of the intersection of a family $\mathcal{F}$ does not depend on the choice of $B \in \mathcal{F}$.

Example 6.8. For any sets A and B:

- $\bigcap_{C \in \{A,B\}} C = A \cap B$.
- $A \cap A = A$.
- $A \cap \emptyset = \emptyset$.
- $\{1, 2\} \cap \{2, 3\} = \{2\}$.
- If for each $n \in \mathbb{N}$, A_n is a set, and $\mathcal{F}$ is a set of the form $\{A_0, A_1, ...\}$, then $\bigcap_{A \in \mathcal{F}} A$ is sometimes written as $A_0 \cap A_1 \cap ...$, or $\bigcap_{n=0}^{\infty} A_n$, and is the set of elements that are in A_n for all $n \in \mathbb{N}$.

Here, lecture 7 ended and lecture 8 started.

Another natural construction would be to replace the "for all $A \in \mathcal{F}$" above by "there exists $A \in \mathcal{F}$". Such a construction is called the *union* of a family of sets. For example, $A \cup B$ would be the sets of objects that are either in A or in B. However, it never appears in the axioms stated so far that this should be a set. Thus we make it a new axiom:

Axiom 6.9 (Union axiom)**.** (U): For any two sets A and B, we can form a set C such that $c \in C$ exactly if $c \in A$ or $c \in B$. C is called the *union* of A and B and we write $C = A \cup B$. More generally, for any family $\mathcal{F}$ of sets, we can form a set C such that $c \in C$ exactly if there exists $A \in \mathcal{F}$ such that $c \in A$. We call C the *union* of the family $\mathcal{F}$ and write $C = \bigcup_{A \in \mathcal{F}} A$.

Example 6.10. If $\mathcal{F} = \{\{0\}, \{0,1\}, \{0,1,2\}, ...\}$ (it turns out that, assuming more axioms, it is a set), then $\bigcup_{A \in \mathcal{F}} A = \{0\} \cup \{0,1\} \cup \{0,1,2\} \cup ... = \mathbb{N}$. Even though we will only be able to make this precise and prove it once we have a definition of the natural numbers, you should be able to convince yourself that this is true: given any element in the union, it has to be in some $\{0,1,2,...,n\}$, for n a natural number, and some must be a natural number $\leq n$. This shows the left hand side is contained in the right hand side. Now given a natural number n, n is in $\{0,1,2,...,n\}$ which is part of $\mathcal{F}$, hence it is in the union. This shows the right hand side is contained in the left hand side.

Theorem 6.11. Let $\mathcal{F}$ be a non-empty family of sets. Let $B \in \mathcal{F}$.

- $B \subseteq \bigcup_{A \in \mathcal{F}} A$.
- $\bigcap_{A \in \mathcal{F}} A \subseteq B$.

Proof. For the first statement, take $b \in B$ arbitrary. We show that $b \in \bigcup_{A \in \mathcal{F}} A$. By definition of the union, we have to see there exists $A \in \mathcal{F}$ such that $b \in A$. We take $A = B$, and since we assumed $B \in \mathcal{F}$, we are done.

For the second statement, let $b \in \bigcap_{A \in \mathcal{F}} A$ be arbitrary. By definition of the intersection, b is in all $A \in \mathcal{F}$, so in particular, $b \in B$, as needed. □

For more practice in showing inclusions, we prove a distributive law for sets:

Theorem 6.12. For any sets A, B, C, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof. By Theorem 6.6, it is enough to show double inclusion: the left hand side is contained in the right hand side, and the right hand side is contained in the left hand side.

We first show the left hand side is contained in the right hand side. Let $x \in A \cap (B \cup C)$ be arbitrary. Then x is in A, and x is in $B \cup C$. We consider two cases: either $x \in B$, or $x \in C$. If x is in B, then x is in A and B, so in $A \cap B$, so in $(A \cap B) \cup (A \cap C)$. If x is in C, then x is in A and C, so in $A \cap C$, so in $(A \cap B) \cup (A \cap C)$.

We now show the right hand side is contained in the left hand side. Let $x \in (A \cap B) \cup (A \cap C)$ be arbitrary. Then x is either in $A \cap B$ or in $A \cap C$. We consider two cases depending on which happens. If x is in $A \cap B$, then x is in A and in B, so x is in A and in $B \cup C$, so $x \in A \cap (B \cup C)$. If x is in $A \cap C$, then x is in A and in C, so in A and in $B \cup C$, so in $A \cap (B \cup C)$.

We have shown that the left hand side and the right hand side are subsets of each other, so they must be equal. □

Using the union axiom, we can form sets with more than two objects. Suppose a, b, c are objects. By pairing, we can form the sets $\{a, b\}$ and $\{b, c\}$. We can then take the union of the sets to obtain the set $\{a, b, c\}$. We can of course iterate this process to build sets with more elements. Even then, it is not clear how to build sets with infinitely many elements, so we add another *axiom*:

Axiom 6.13. (R): The real numbers form a set. We call this set $\mathbb{R}$.

Finally, we also have to define another operation on sets:

Axiom 6.14 (The power set axiom)**.** ($\mathcal{P}$): For any set A, there exists a set B whose elements are exactly the subsets of A: $x \in B$ if and only if $x \subseteq A$. We write $B = \mathcal{P}(A)$ and call B the *power set* of A.

Example 6.15. $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

We now have that $\mathcal{P}(\mathbb{R})$, $\mathcal{P}(\mathcal{P}(\mathbb{R}))$, ... are all sets, and we can also take their union or use the axiom of separation to restrict them to what we want. This basically shows that any collection (in the informal sense) of objects we are likely to care about will be a set, so we adopt the following principle:

Fact 6.16. Any collection of real numbers, sets of real numbers, sets of sets of real numbers, etc. is a set. Also, any finite collection of objects is a set.

In short, unless you really exaggerate, any collection you are likely to build will be a set. Thus we will be careless and won't justify every time exactly why an object we build is a set.

We are now ready to precisely define the set of natural numbers. We intend to build a set X whose elements are 0, 1, 2, 3, 4, ... In particular, we would like that:

(1) $0 \in X$.
(2) For all $x \in \mathbb{R}$, if $x \in X$, then $x + 1 \in X$.

Call such a set an *inductive set*. There are many such sets that are not the natural numbers (for instance, $\mathbb{R}$ itself is such a set). In a sense however, we want the properties above and no more, i.e. we want the natural numbers to be the *smallest* set satisfying those properties. In set-theoretic language, we will take the *intersection* of all sets satisfying those properties.

Definition 6.17. The set $\mathbb{N}$ of natural numbers is defined to be the intersection of all inductive sets (see above). In symbols[13]

$$\mathbb{N} := \bigcap_{A \in \mathcal{F}} A$$

Where

$$\mathcal{F} := \{A \in \mathcal{P}(\mathbb{R}) \mid A \text{ is an inductive set}\}$$

Note first that $\mathcal{F}$ above is non-empty ($\mathbb{R}$ is an inductive set). Moreover, $\mathbb{N}$ is also an inductive set (i.e. it has the properties above). From the definition of the natural numbers and Theorem 6.11, we have that:

Theorem 6.18. If S is an inductive set, then $\mathbb{N} \subseteq S$.

As an exercise in understanding the definition, let's prove an easy property of $\mathbb{N}$:

Theorem 6.19. If x is a negative real number, then $x \notin \mathbb{N}$.

Proof. The set $\mathbb{R}_{\geq 0} = \{y \in \mathbb{R} \mid y \geq 0\}$ is an inductive set that does not contain x. As $\mathbb{N}$ is contained in any inductive set, $\mathbb{N} \subseteq \mathbb{R}_{\geq 0}$, and so $x \notin \mathbb{N}$. □

We can also redefine the integers and rational numbers more precisely:

Definition 6.20.

- The set $\mathbb{Z}$ of *integers* is defined by:

$$\mathbb{Z} := \mathbb{N} \cup \{x \in \mathbb{R} \mid x = -n \text{ for some } n \in \mathbb{N}\}$$

[13]This is yet another example where using symbols makes things harder to understand. In your own writeup, it is perfectly fine if you choose to describe a set in words (e.g. if you say that the set of natural numbers is the intersection of all inductive sets), but you should make sure you are aware of the precise meaning of those words.

- The set $\mathbb{Q}$ of *rationals* is defined by:

$$\mathbb{Q} := \{x \in \mathbb{R} \mid x = n/m \text{ for some } n, m \in \mathbb{Z} \text{ with } m \neq 0\}$$

These definitions in our belt, we are now ready to prove statements about the natural numbers.

7. Induction

We previously got stuck trying to prove that any natural number was either even or odd. What went wrong and what should a proof of this look like? For a start, we know that 0 is even, and we know that if n is even, then $n+1$ is odd, and if n is odd, then $n+1$ is even. Thus 1 is odd, 2 is even, 3 is odd, and so on. This "and so on" is usually a good indication that one has to use the principle of mathematical induction:

Theorem 7.1 (The principle of mathematical induction)**.** Assume $p(x)$ is a propositional function, where the variable x takes values in the natural numbers. Assume we know that:

(1) $p(0)$ is true.
(2) For any natural number n, if $p(n)$ is true, then $p(n+1)$ is true.

Then $p(n)$ is true for all natural numbers n.

Proof. Let S be the set of natural numbers where p holds. In symbols:

$$S := \{n \in \mathbb{N} \mid p(n)\}$$

From the assumptions on p, we know that S is an inductive set, so by Theorem 6.18, $\mathbb{N} \subseteq S$. By definition, $S \subseteq \mathbb{N}$, and so $S = \mathbb{N}$. Thus for any natural number n, $n \in S$, so $p(n)$ is true. □

The principle of mathematical induction tells us that to prove a statement holds of all natural numbers it is enough to prove it holds for 0 (sometimes called the base case), and that it holds for $n+1$ whenever it holds for n (sometimes called the inductive step). When proving $p(n)$ implies $p(n+1)$, $p(n)$ is called the *inductive hypothesis*. The intuitive justification for this principle is the following: assume we know that $p(0)$ holds and $p(n+1)$ holds whenever $p(n)$ holds. Then taking $n = 0$, $p(0+1) = p(1)$ holds. Taking $n = 1$, $p(2)$ holds. Taking $n = 2$, $p(3)$ holds, and so on. One image to have in mind is that of climbing a ladder: to climb an entire ladder, it is enough to start on the first step ($p(0)$), and from step n, move up to step $n+1$.

We are finally ready to prove Fact 5.8.

Theorem 7.2. Any natural number is either even or odd.

Proof. We use the principle of mathematical induction on the propositional function $p(x)$ saying "x is either even or odd".
Base case. $p(0)$ holds, since $0 = 2 \cdot 0$, so is even.
Inductive step. We want to show that for any natural number n, $p(n)$ implies $p(n+1)$. Recall from the section on direct proofs that to do this we have to take an arbitrary natural number n, and show assuming $p(n)$ is true that $p(n+1)$ is true. So take an arbitrary natural number n, and assume $p(n)$ is true, i.e. n is either even or odd. If n is even, then $n+1$ is odd, so $p(n+1)$ holds. If n is odd, then $n+1$ is even, so $p(n+1)$ holds. Thus in both cases, $p(n+1)$ holds.

Therefore by the principle of mathematical induction $p(n)$ holds for any natural number n, i.e. any natural number is either even or odd. □

Since it is easy to make mistakes while using the principle of mathematical induction, I strongly recommend you to format your proof according to the basic template above, namely:

(1) Say that you are going to use the principle of mathematical induction (or just induction) and explicitly state the propositional function $p(x)$ you are going to use it with.
(2) Make a subsection for the base case, and give its proof.
(3) Make a subsection for the inductive step, and give its proof.
(4) Conclude by quoting the principle of mathematical induction.

Here, lecture 8 ended and lecture 9 started.

Theorem 7.3. Any integer is either even or odd.

Proof. Let x be an integer. Then x is either a natural number (in which case we use the previous theorem), or $x = -n$ for some natural number n. Pick such an n. By the previous theorem, n is either even or odd. If it is even, then $-n$ will be even, and if it is odd, then $-n$ will be odd (Theorem 5.5). Therefore x is either even or odd. □

The principle of mathematical induction similarly applies if we start somewhere else than 0. For example, if we prove only that $p(1)$ and $p(n)$ implies $p(n+1)$ for $n \geq 1$, then we get that $p(n)$ holds for all natural numbers $n \geq 1$. More generally:

Theorem 7.4 (The generalized principle of mathematical induction)**.** Assume m is an integer. Assume $p(x)$ is a propositional function, where the variable x takes values in the integers $\geq m$. Assume we know that:

(1) $p(m)$ is true.
(2) For any integer $n \geq m$, if $p(n)$ is true, then $p(n+1)$ is true.

Then $p(n)$ is true for any integer $n \geq m$.

Proof. Consider the propositional function $q(x)$ (where x is a natural number) which says that $p(x + m)$ is true. Then $q(0)$ is the same as $p(m)$ which is true by assumption, and for any natural number n, if $q(n)$ holds, then $p(n + m)$ holds, so $p(n + m + 1)$ holds, so $q(n + 1)$ holds. By the principle of mathematical induction, $q(n)$ holds for all natural numbers n, and hence $p(n + m)$ holds for all natural numbers n, so in other words, $p(n)$ holds for all natural numbers $n \geq m$. □

We now turn to *inductive definitions*. We would like to make sense of objects such as the sum $0 + 1 + 2 + \ldots + n$, where n is a natural number, or the product $x \cdot x \cdot \ldots \cdot x$ (n times). Again, we want to get rid of the ambiguities raised by the three dots. For this, we introduce new notation:

Definition 7.5. For n a natural number and x a real number, we *inductively* define x^n as follows:

- $x^0 = 1$.
- $x^{n+1} = x^n \cdot x$.

Remark 7.6. We have defined $0^0 = 1$. It turns out to be a very useful convention, but there are some issues with giving a definite value to 0^0. For example, the functions 0^x and x^0 have limits 0 and 1 respectively as x approaches 0 from the right (this is why 0^0 is typically an undeterminate form in calculus textbooks). This shows that one must in general be careful when dealing with exponentiation, limits, and the number zero. In this course, we shall be safe, as we will not deal with limits.

Fully justifying why this style of definition is permissible would take us too far, but you can think of it as a consequence of the principle of mathematical induction: we know that x^n is defined for $n = 0$, and we know that if x^n, then x^{n+1} is defined. Therefore x^n is defined for all natural numbers n. The definition is not circular, since we are only relying on the definition at stage n to define stage $n+1$ (i.e. we always rely on past stages, never on current or future stages).

Note that $x^2 = x^1 \cdot x = x^0 \cdot x \cdot x = x \cdot x$, so this agrees with our previous definition of the square of a number.

Let's look at how we would do the same thing for sums:

Definition 7.7 (Σ notation)**.** Assume $f(i)$ is some expression[14] depending on i, and n is a natural number. We define $\sum_{i=1}^{n} f(i)$ as follows:

- $\sum_{i=1}^{n} f(i) = 0$ if $n = 0$.

[14]We will later introduce the concept of a function and make this precise.

- $\sum_{i=1}^{n+1} f(i) = f(n+1) + \sum_{i=0}^{n} f(i)$.

We can similarly define $\sum_{i=k}^{n} f(i)$ for k a natural number. If $k > n$, we adopt the convention that this is zero.

Remark 7.8. It is sometimes simply more convenient to write three dots instead of introducing new notation. We may in the future do so, but you should keep in mind that this is only a *convenience*, and that this could be made precise using induction. Sometimes, we may also need to be absolutely clear and avoid using the three dots. In your own writing, you should use your own judgment as to which is best: a more readable notation, or a more precise one?

Example 7.9.

- $\sum_{i=1}^{n} 1 = 1 + 1 + 1 + \ldots + 1 = n$ (the ones repeat n times).
- $\sum_{i=1}^{n} i = 1 + 2 + 3 + \ldots + n$.

Is there a simple formula giving us the value of $\sum_{i=1}^{n} i$? It turns out there is:

Theorem 7.10. For any natural number n:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Proof. We use the principle of mathematical induction on the propositional function $p(x)$ saying "$\sum_{i=1}^{x} i = \frac{x(x+1)}{2}$".
Base case. If $p(0)$ just says that $\sum_{i=1}^{0} i = 0$. This is true since the left hand side is zero by definition.
Inductive step. Let n be an arbitrary natural number, and assume $p(n)$ holds, i.e. $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. We want to see that the same formula holds with n replaced by $n+1$, namely $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$. We compute:

$$\sum_{i=1}^{n+1} i = n+1+\sum_{i=1}^{n} i = n+1+\frac{n(n+1)}{2} = \frac{2(n+1)+n(n+1)}{2} = \frac{(n+2)(n+1)}{2}$$

Where the first equality uses the definition of Σ notation, the second uses the *inductive assumption* $p(n)$, and the last two hold by some elementary algebra (that could easily be justified from the facts we know about the real numbers). This completes the proof of the inductive step.

By the principle of mathematical induction, $p(n)$ holds for any natural number n, as desired. □

7.1. **Strong induction.** In the inductive step of a proof by induction we have to prove $p(n+1)$ holds assuming $p(n)$. Wouldn't it be nice if we could assume that $p(k)$ for $k \leq n$ also holds? Since we think of proving something by induction as climbing a ladder, and we have already climbed all steps $\leq n$ before reaching step $n+1$, this sounds reasonable. This is what the principle of strong induction tells us:

Theorem 7.11 (The principle of strong induction)**.** Assume $p(x)$ is a propositional function, where the variable x takes values in the natural numbers. Assume we know that:

(1) $p(0)$ is true.
(2) For any natural number $n \geq 1$, if $p(m)$ is true for any natural number $m < n$, then $p(n)$ is true.

Then $p(n)$ is true for all natural numbers n.

Proof. We use the principle of mathematical induction on the proposition $q(x)$ which says "$p(m)$ is true for any natural number $m \leq x$".
Base case. $q(0)$ just says that $p(x)$ is true for any natural number $m \leq 0$, but since the only such natural number is zero, it is enough to see that $p(0)$ is true, and it is by assumption.
Inductive step. Let n be an arbitrary natural number, and assume $q(n)$ holds. We show $q(n+1)$, i.e. $p(m)$ holds for all $m \leq n+1$. The induction hypothesis $q(n)$ already tells us that $p(m)$ holds for every $m \leq n$, so it is enough to see that $p(n+1)$ holds. But this is the case by assumption (2). Therefore $q(n+1)$ is true.

By the principle of mathematical induction, $q(n)$ is true for all natural numbers n. In particular, $p(n)$ is true for all natural numbers n. □

Remark 7.12. We can combine the two conditions of the principle of strong induction into only one: For any natural number n, if $p(m)$ is true for all $m < n$, then $p(n)$ is true. This is the same as (2) if $n \geq 1$, and if $n = 0$, then the statement "$p(m)$ is true for any natural number $m < 0$" is always *vacuously true*, i.e. it holds simply because there is no natural number below 0.

As an application of the principle of strong induction, we prove that every natural number is a product of primes.

Definition 7.13. An integer m *divides* an integer n (written $m|n$) if there exists an integer k such that $n = mk$.

Here are some easy properties of dividing:

Theorem 7.14. For all integers n, m, k:

(1) n is even if and only if 2 divides n.
(2) If $n = m \cdot k$, then both m and k divide n.
(3) For m nonzero, m divides n if and only if n/m is an integer.
(4) m divides 0.
(5) 1 divides n.
(6) 0 divides n if and only if $n = 0$.
(7) m divides n if and only if $\pm m$ divides $\pm n$.
(8) If m divides n and n is nonzero, then $|m| \leq |n|$.
(9) If k divides m and m divides n, then k divides n.

Proof.

(1) By definition.
(2) By definition.
(3) If m divides n, there exists an integer r such that $n = mr$, so since m is nonzero, $r = n/m$, so n/m is an integer. Conversely, if n/m is an integer r, then $mr = n$, so m divides n.
(4) $0 = 0 \cdot m$.
(5) $n = 1 \cdot n$.
(6) If 0 divides n, then $n = r \cdot 0 = 0$ for some integer r. Conversely, by (4) any integer divides 0, and so in particular 0 divides 0.
(7) If m divides n, then $n = mr$ for some integer r. Thus $-n = m(-r)$, so m divides $-n$, and also $n = (-m)(-r)$, so $-m$ divides n. This shows one can change the signs of m and n arbitrarily without changing divisibility, and the result follows. This also proves the converse.
(8) Assume m divides n and n is nonzero. By (7), we can replace n and m by their absolute value, so assume that n and m are already natural numbers. Fix an integer r such that $n = mr$. Since n is nonzero, both r and m are nonzero. Since n and m are natural numbers, r is a natural number, so must be positive. Thus we have $1 \leq r = n/m$, so multiplying by m, $m \leq n$, as needed.
(9) Assume k divides m and m divides n. Fix integers m' and n' such that $m = km'$ and $n = mn'$. Then $n = k(n'm')$, so k divides n.

□

Here, lecture 9 ended and lecture 10 started

Definition 7.15. A natural number p is *prime* if $p \geq 2$ and if any natural number that divides p is either 1 or p. A natural number ≥ 2 which is not prime is called *composite*.

Example 7.16. You should convince yourself that 2 and 3 are prime, but 4 is not prime, as $4 = 2 \cdot 2$, so 2 divides 4. The next primes are $5, 7, 11, 13, \ldots$. We will see that there are infinitely many primes.

Theorem 7.17. A natural number $n \geq 2$ is composite if and only if there exists natural numbers m and k with $1 < k \leq m < n$ and $n = m \cdot k$.

Proof. If there exists m and k with $1 < k \leq m < n$ and $n = mk$, then they witness that n is composite. Conversely, if n is composite, there exists a natural number m that is not 1 or p and divides n. Since n is nonzero and both n and m are natural numbers, Theorem 7.14.(8) tells us that $m \leq n$. By assumption, $m \neq 1$, $m \neq n$, so $1 < m < n$. Since m divides n, $k := n/m$ is a natural number and it is easy to check that $1 < k < n$. Exchanging the role of m and k if necessary, we can assume without loss of generality that $k \leq m$. □

Theorem 7.18. Let $n \geq 2$ be a natural number. Then n is a product of primes, i.e. there exists a natural number r, and primes $p_0, \ldots, p_r$ such that $n = p_0 p_1 \cdots p_r$.

Proof. We use the principle of strong induction on the proposition $p(x)$ which says that x is a product of primes. We start our induction at $x = 2$ and prove $p(x)$ holds for every natural number $x \geq 2$.
Base case. $p(2)$ holds since 2 is prime.
Inductive step. Let n be an arbitrary natural number, $n > 2$. Assume $p(m)$ holds for every $m < n$. If n is prime, we are done. If n is not prime, we use the previous theorem to see that there exists natural numbers k and m with $1 < k \leq m < n$ so that $n = m \cdot k$. By the induction hypothesis, $p(m)$ and $p(k)$ hold, so $m = p_0 \cdots p_l$ and $k = p_{l+1} \cdots p_r$ for primes $p_0, \ldots, p_l, \ldots, p_r$. Therefore $n = m \cdot k = p_0 \cdots p_r$ is also a product of primes.

By the principle of strong induction, every natural number $n \geq 2$ is a product of prime. □

Remark 7.19. In this sense, the primes are the building blocks of the natural numbers. We will see later that this decomposition into primes is unique (up to the ordering of the primes).

Example 7.20. $4 = 2 \cdot 2$ (so the same prime may appear several times in the decomposition). $10 = 2 \cdot 5$, $150 = 2 \cdot 3 \cdot 5 \cdot 5$.

To continue, we need the concept of a minimal element

Definition 7.21. Assume $a \in \mathbb{R}$ and $X \subseteq \mathbb{R}$. a is a *minimal element (or minimum)* of X if $a \in X$ and for any $b \in X$, $a \leq b$.

Example 7.22.

- The set $\mathbb{Z}$ has no minimal elements: if $a \in \mathbb{Z}$, $b := a - 1$ is strictly smaller.
- The set $\mathbb{R}_{>0}$ of positive real numbers has no minimal elements: If $a \in \mathbb{R}_{>0}$, then $a/2$ is strictly smaller.
- The set $\mathbb{R}_{\geq 0}$ has minimal element 0.

Remark 7.23. If $X \subseteq \mathbb{R}$ has a minimal element a, then it is unique: if $a' \in X$ is a minimal element, then $a \leq a'$ and $a' \leq a$ by definition of a minimal element, and so $a = a'$.

As another application of strong induction, you will prove in your homework:

Theorem 7.24 (The well-ordering principle)**.** Any non-empty subset of $\mathbb{N}$ has a minimal element.

We will use it to prove Fact 5.10. In fact, we will prove more:

Definition 7.25. Two integers n and m are called *coprime* if no prime divides both n and m.

Example 7.26.

- If n and m are even, then they are not coprime, as the prime 2 divides both of them.
- If p and q are distinct primes, then p and q are coprime.
- 8 and 15 are coprime (you can check it by trying all the primes below 8), even though they are not prime (2 divides 8, 3 divides 15).
- 6 and 15 are not coprime, as 3 divides both of them.

Fact 5.10 follows from:

Theorem 7.27. Given a rational number r, there exists coprime integers n and m with m nonzero such that $r = n/m$.

Proof. It is enough to prove it for non-negative rational numbers (if $r < 0$, use the result on $-r$ and use that the dividing relation is insensible to change of signs). Let r be a non-negative rational number. By the well-ordering principle, find natural numbers m and n with m nonzero such that $r = n/m$ and $n + m$ is minimal (formally, we consider the set of natural numbers x for which there exists natural numbers n and m such that $x = n + m$ and $r = n/m$, use the well ordering principle to pick a minimal element x of this set, and then pick n and m with $x = n + m$). We claim that n and m are coprime. Assume for a contradiction they are not. Then there exists a prime p that divides n

and m. Let $n' := n/p$, $m' := m/p$. Since $p \geq 2$, $n' < n$, $m' < m$, so $n'+m' < n+m$ and $r = n/m = n'/m'$. This contradicts the minimality of $n + m$.

□

8. Set theory

Now that we have some basic understanding of proofs, it is worth spending some time studying sets further. One of our first goals is to define the notion of a function: In a calculus course, a function is usually defined as a rule associating each object in its domain to another. This is a somewhat imprecise definition, and we will do much better in this chapter. Once functions have been properly defined, we will be able to use them to put sets in one-to-one correspondence, and make sense of the *size* of a set. This will work even for infinite sets, and will lead us to see that there are different "sizes" of infinity!

8.1. **Functions and relations.**

8.1.1. *Ordered pairs.* We start by defining the notion of an *ordered* pair. Recall that sets are unordered: for two objects a and b, $\{a, b\} = \{b, a\}$. We now define a notion of pairing such that the order matters:

Definition 8.1. For objects a and b, the *ordered pair* (a, b) is an object such that for any two other objects c and d, $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

Remark 8.2. It is rather unfortunate that in calculus and analysis, the notation (a, b) for real numbers a and b also denotes the open interval with endpoints a and b. It is usually clear from context which of the two is meant though.

Surprisingly, it turns out sets can be used to code ordered pairs: you will see in your homework that for objects a and b, the set $\{\{a\}, \{a, b\}\}$ is a good way to code the pair (a, b). Using this definition and iterating the power set axiom as many times as necessary, it is not too hard to see the following:

Fact 8.3. Assume A and B are sets. Then there exists a set C whose elements are exactly the ordered pairs (a, b) with $a \in A$ and $b \in B$. We call C the *cartesian product* of A and B, and write $C = A \times B$.

Example 8.4.

- $\mathbb{R} \times \mathbb{R}$ (sometimes also written $\mathbb{R}^2$) is the set of all pairs of real numbers. We can see a pair of real numbers as giving the

coordinates of a point in the plane, so we sometimes just call $\mathbb{R}^2$ the plane.
- For any set A, $\emptyset \times A = A \times \emptyset = \emptyset$.
- $\{1,2\} \times \{3,4\} = \{(1,3),(1,4),(2,3),(2,4)\}$.
- As the example above shows, in general, $A \times B \neq B \times A$, as $(1,3) \in \{1,2\} \times \{3,4\}$ but $(1,3) \notin \{3,4\} \times \{1,2\}$. This case shows that we can even have $(A \times B) \cap (B \times A) = \emptyset$.

Here, lecture 10 ended and lecture 11 started.

8.1.2. *Relations.* There are many ways to compare two real numbers x and y: we can ask whether $x \leq y$, whether $x = y^2$, whether $x \neq y$, whether x or y is an integer, etc. More generally, a relation on $\mathbb{R}$ is simply a way to compare x and y. Now that we have the notion of ordered pairs, we can make this precise:

Definition 8.5. Let A and B be sets. A *relation* R on $A \times B$ is a subset of $A \times B$. If $B = A$, we say R is a relation on A.

Notation 8.6. For R a relation on $A \times B$, and $x \in A$, $y \in B$, we think of x and y as being related if $(x,y) \in R$, and write xRy (read "x is related to y") for $(x,y) \in R$.

Example 8.7.

(1) The set $R := \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$ is a relation and xRy if and only if $x \leq y$. We can even see $\leq$ as being R itself.
(2) The set $G := \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$ is a relation. This is a special one, since every $x \in \mathbb{R}$ has exactly one y related to it. We will end up calling such relations *functions*.

8.1.3. *Equivalence relations.* Here are some structural properties relations can have:

Definition 8.8. A relation R on a set A is called:

(1) *Reflexive* if for any x in A, xRx.
(2) *Symmetric* if for any x and y in A, xRy implies yRx.
(3) *Transitive* if for any x, y, and z in A, xRy and yRz imply xRz.

Example 8.9. Take $A = \mathbb{R}$. The relation $\leq$ is reflexive and transitive but is not symmetric (as $0 \leq 1$ but $1 \not\leq 0$). The relation $<$ is transitive but not reflexive and not symmetric. The relation xRy if and only if $y = x^2$ is not reflexive ($2 \neq 2^2$), not transitive ($16 = 4^2$, $4 = 2^2$, but $16 \neq 2^2$), and not symmetric ($4 = 2^2$ but $2 \neq 4^2$). The equality relation is reflexive, symmetric, and transitive.

In a sense, relations that satisfy the three properties above look like the equality relation. We give such relations a name:

Definition 8.10. A relation R on a set A which is reflexive, symmetric, and transitive is called an *equivalence relation on* A.

Equivalence relations appear in many different parts of mathematics and computer science. They are a witness to the power one gets by generalizing many different cases into one.

Example 8.11.

(1) As already observed, for any set A, equality on A (i.e. $\{(x, x) \in A \times A \mid x \in A\}$) is an equivalence relation on A.
(2) Take A to be the set of integers, and let n be an integer. Say xEy if and only if n divides $x-y$. This is an equivalence relation. When xEy, we write $x \equiv y \bmod n$, and say x *is congruent to* y *modulo* n. For $n = 0$, we obtain regular equality: $x \equiv y \bmod 0$ if and only if $x = y$, and for $n = 1$ (or $n = -1$), we obtain that everything is equivalent: For any integer x and y, $x \equiv y \bmod 1$. For $n = 2$, we get that $x \equiv 0 \bmod 2$ if and only if x is even, and $x \equiv 1 \bmod 2$ if and only if x is odd.
(3) For $A = \mathcal{P}(\mathbb{N})$, say xEy if and only if x and y have the same finite number of elements (this will be defined precisely later), or x and y are both infinite. This is an equivalence relation.
(4) Take A to be the set of CMU students, and say xEy if and only if x and y have the same first name. This is an equivalence relation.

8.1.4. *Functions.*

Definition 8.12. A relation f on a set $A \times B$ (together with A and B) is called a *function* if for every $x \in A$, there is a unique $y \in B$ such that $(x, y) \in f$. In this case, we write $y = f(x)$. We call A the *domain* and B the *codomain* of f, and write $f : A \to B$ (said "f is a function from A to B") to say that f is a function with domain A and codomain B.

Remark 8.13. In calculus, it is customary to define functions by saying something like "Let $f : A \to B$ be the function defined by $f(x) = E(x)$", where E is some expression defining the function. This is fine, but there are many other ways to define functions. For example, one can write it as an explicit set, or one can just use words to describe what it does.

Remark 8.14. *The domain and codomain are part of the function*, so for example the functions $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ and $g : \mathbb{R} \to \{x \in \mathbb{R} \mid x \geq 0\}$ defined by $g(x) = x^2$ are different as they do not have the same codomain.

Example 8.15.

- The relation $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$ defines a function from $\mathbb{R}$ to $\mathbb{R}$.
- The relation $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$ does not define a function, as for a given x, there are many y such that $x \leq y$ (for example x or $x + 1$)
- The relation $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y^2\}$ does not define a function, since for a negative x, there is no y such that $x = y^2$, and for positive x, there are two different y such that $y^2 = x$ (namely $\sqrt{x}$ and $-\sqrt{x}$) If one restricts x and y to lie in the set $\mathbb{R}_{\geq 0}$ of non-negative real numbers, one obtains the function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ given by $f(x) = \sqrt{x}$.
- Another example of a function is the map[15] $f : \mathbb{R} \to \mathbb{R}$ given by

$$f(x) = \begin{cases} 1 & \text{if } x \text{ is rational} \\ 0 & \text{if } x \text{ is irrational} \end{cases}$$

- Functions don't have to have sets of numbers as domain or codomain. For example one can define a function f mapping the set S of days of the week to itself, by $f(x) =$ the day after x (so for example $f(\text{Sunday}) = \text{Monday}$). Another example: take $A = \{a, b, c\}, B = \{c, d\}$ and define $f : A \to B$ by $f(a) = c, f(b) = f(c) = d$.
- A weird consequence of the definition: For any set B, there is a unique function $f : \emptyset \to B$, the "empty" function, which is just the empty set! Also, if $f : A \to \emptyset$, then we must have $A = \emptyset$ (if A were non-empty, there would be nowhere to send the elements of A to!).
- Given a set A, the function $f : A \to A$ defined by $f(x) = x$ is called the *identity function.*
- We can see a propositional function $p(x)$ with domain of discourse A as a function from A to $\{F, T\}$ that to each member a of A associates the truth value of the proposition $p(a)$.

8.1.5. *Some operations on functions.*

Definition 8.16 (Image and inverse image)**.** Let A and B be sets and $f : A \to B$ be a function.

(1) For $C \subseteq A$, The *image of C under f*, written $f[C]$ is the set $\{b \in B \mid \text{there exists } c \in C \text{ such that } f(c) = b\}$. The *range* of f is $f[A]$.

[15] "map" and "function" are synonymous.

(2) For $C \subseteq B$, the *inverse image of C under f*, written $f^{-1}[C]$ is the set $\{a \in A \mid f(a) \in C\}$.

Example 8.17. The range of the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is all the non-negative real numbers. The range of the function $g : \mathbb{R} \to \mathbb{R}$ which is 1 if the input is rational and 0 otherwise is $\{0, 1\}$. The inverse image of $\{1/2\}$ under this function is the empty set, and the inverse image of $\{0\}$ under this function is the set of irrational numbers. For x a non-negative number, the inverse image of $\{x\}$ under f is $\{-\sqrt{x}, \sqrt{x}\}$.

Here, lecture 11 stopped and lecture 12 started.

Definition 8.18 (Composition of functions)**.** Let A, B, C be sets and $f : A \to B$, $g : B \to C$ be functions. The *composition* of f and g (written $g \circ f$) is the function $h : A \to C$ defined by $h(a) = g(f(a))$.

Example 8.19.

(1) The composition of the functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ and $g(x) = x + 1$ is $(g \circ f)(x) = g(f(x)) = g(x^2) = x^2 + 1$. In contrast, $(f \circ g)(x) = f(x + 1) = (x + 1)^2$, so even if domains and codomains are all the same, $f \circ g \neq g \circ f$.
(2) The composition of any function $f : A \to B$ with the identity g on B (recall that the identity is the function that sends every element to itself) is just $(g \circ f)(x) = f(x)$, so $g \circ f = f$.

8.2. **Cardinalities.** We have seen that given a function $f : A \to B$, it was possible that some elements in B were not the image of any element in A, or that distinct elements in A mapped to the same element in B. When this does not happen, the function is easier to understand, and we give these conditions names:

Definition 8.20 (Injection, surjection, bijection)**.** Assume A and B are sets and $f : A \to B$ is a function.

- f is a *surjection* (we also say f is *surjective*) if for every $b \in B$, there exists $a \in A$ such that $f(a) = b$.
- f is an *injection* (we also say f is *injective*) if for every a and a' in A, $f(a) = f(a')$ implies $a = a'$.
- f is a *bijection* (we also say f is *bijective*) if it is both an injection and a surjection.

An injection is a function that sends distinct elements in its domain to distinct elements in its codomain, while a surjection covers the entire codomain of the function. The definition of a bijection makes precise the notion of "one to one correspondence".

Example 8.21.

(1) The map $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is not a bijection: it is neither injective nor surjective. It is not injective because $f(-1) = f(1)$ (so distinct members of the domain can get sent to the same element), and it is not surjective because there is no real number x such that $f(x) = -1$.
(2) On the other hand, the map $g : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ defined by $g(x) = x^2$ *is* a bijection: it is injective: if $a, a' \in \mathbb{R}_{\geq 0}$ and $f(a) = f(a')$, then $a^2 = (a')^2$, and since they are both non-negative, uniqueness of the square root gives us that $a = a'$. It is surjective: given a non-negative b, one can take $a := \sqrt{b}$, and then $f(a) = b$.
(3) Let $A := \{1, 2, 3\}$, $B := \{2, 4\}$. The map $f : A \to B$ given by $f(1) = f(2) = 2$ and $f(3) = 4$ is a surjection that is not an injection. The map $g : B \to A$ given by $g(2) = 1$, $g(4) = 2$ is an injection that is not a surjection.

Theorem 8.22. $f : A \to B$ is a bijection if and only if for each $b \in B$ there is a unique $a \in A$ such that $f(a) = b$.

Proof. Assume f is a bijection. Let $b \in B$. Since f is a surjection, there is $a \in A$ such that $f(a) = b$. a is unique: if $a' \in A$ is such that $f(a') = b$, then $f(a) = f(a')$, so since f is injective, $a = a'$.

Conversely, assume that for every $b \in B$ there is a unique $a \in A$ such that $f(a) = b$. Then in particular f is surjective. To see f is injective, assume $a, a' \in A$ and $f(a) = f(a')$. There is a unique a'' such that $f(a'') = f(a)$, so $a'' = a = a'$, as needed. □

Bijections are a particularly nice class of functions. For a start, one can start from a bijection, and produce an *inverse*:

Definition 8.23. Given a bijection $f : A \to B$, the *inverse* of f is the function $g : B \to A$ that to each $b \in B$ associates the unique $a \in A$ so that $f(a) = b$. We write $g = f^{-1}$.

Remark 8.24. For any (not necessarily bijective) function $f : A \to B$ and any $C \subseteq B$, the *inverse image* $f^{-1}[C]$ is always defined, even though the function f^{-1} itself need not be.

Example 8.25.

- The inverse of the map $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ given by $f(x) = x^2$ is $f^{-1}(x) = \sqrt{x}$.
- The map $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ given by $f(x) = \frac{1}{x}$ is a bijection (exercise), and $f^{-1} = f$.

- The inverse of the map $f : \{1, 2, 3\} \to \{4, 5, 6\}$ given by $f(1) = 1$, $f(2) = 6$, $f(3) = 5$ is given by $f^{-1} : \{4, 5, 6\} \to \{1, 2, 3\}$ defined as $f^{-1}(6) = 2$, $f^{-1}(5) = 3$, $f^{-1}(1) = 1$.
- Assume A is the set of days of the week. The map f that maps each day to the next one is a bijection (why?), and its inverse maps each day of the week to the preceeding one.

Theorem 8.26. Assume $f : A \to B$ is a bijection. Then f^{-1} is a bijection.

Proof. Exercise. □

8.2.1. *Cardinalities of sets.* If two sets A and B contain 5 elements, say $A = \{a_1, ..., a_5\}$, $B = \{b_1, ..., b_5\}$, we can build a bijection from A to B that sends a_i to b_i for each $1 \leq i \leq 5$. Conversely, if A has 6 elements and B has 5 elements, we expect not to be able to put A and B in one to one correspondence. This motivates the following definition:

Definition 8.27. Two sets A and B are said to *have the same cardinality* or to be *equipotent* if there is a bijection $f : A \to B$.

Theorem 8.28. Let U be a set. The relation E on $\mathcal{P}(U)$ defined by xEy if and only if x and y are equipotent is an equivalence relation.

Proof. Exercise. □

Definition 8.29. For n a natural number, we define the set $[n]$ to be $\{1, 2, ..., n\}$. More precisely, $[n] := \{m \in \mathbb{N} \mid 1 \leq m \leq n\}$ (so $[0] = \emptyset$). For n a negative integer, we also define $[n] = \emptyset$.

We now prove the seemingly obvious, but crucial:

Theorem 8.30. Assume n and m are natural numbers. Then $[n]$ and $[m]$ are equipotent if and only if $n = m$.

Proof. If $n = m$, then the identity function $f : [n] \to [n]$ defined by $f(x) = x$ is a bijection from $[n]$ to $[n]$ (exercise).

For the converse, we use induction on the propositional function $p(x)$ which says "If f: $[m] \to [x]$ is a bijection, then $m = x$".
Base case. If $n = 0$, then since the only function with codomain the empty set is the empty function we must have $f : \emptyset \to \emptyset$ so $m = 0 = n$.
Inductive step. Assume $p(n)$ holds. Assume $f : [m] \to [n + 1]$ is a bijection, and we have to show $m = n + 1$. Notice that $m > 0$, as the only bijection with empty domain is the empty bijection, so $m = 0$ would imply $n+1 = 0$, which is impossible. Let $r := f^{-1}(n+1)$. Define the function $g : [m - 1] \to [n]$ by

$$g(k) = \begin{cases} f(k) & \text{if } k < r \\ f(k+1) & \text{if } k \geq r \end{cases}$$

First observe that the codomain of g is indeed $[n]$, since $g(k) \neq f(r) = n+1$ for any k. We claim that g is a bijection. It is injective: if $g(k) = g(k')$, assume without loss of generality that $k \leq k'$. Then either $f(k) = f(k')$ or $f(k+1) = f(k'+1)$ in which case $k = k'$, or $f(k) = f(k'+1)$, so $k = k'+1$, which is impossible since we assumed $k \leq k'$. g is also surjective: given $b \in [n]$, use surjectivity of f to find $a \in [m]$ such that $f(a) = b$. Now let k be a if $a < r$, or $a - 1$ if $a \geq r$. Then it is easy to check that $g(k) = f(a) = b$, as needed.

Since g is a bijection, by the induction hypothesis, $m - 1 = n$, so $m = n + 1$. □

Theorem 8.31. Assume A is a set and n, m are natural numbers such that A is equipotent to $[n]$ and $[m]$. Then $n = m$.

Proof. Exercise. □

Thus we see that a set can be equipotent to *at most one* $[n]$. We can now define precisely what it means for a set to have n elements.

Here, lecture 12 stopped and lecture 13 started.

Definition 8.32. For n a natural number, a set A is said to have *cardinality* n or to *have* n *elements* (written $|A| = n$) if A and $[n]$ are equipotent.

We say A is *finite* if there is a natural number n such that $|A| = n$. We say A is *infinite* if it is not finite.

Remark 8.33. If A is infinite, we will *not* define what $|A|$ means, but given another set B, we can still ask whether A and B have the same cardinality.

Example 8.34.

(1) $|\emptyset| = 0$, and more generally for a natural number n, $|[n]| = n$.
(2) $\mathbb{N}$ is infinite. To see this, assume for a contradiction that $f : \mathbb{N} \to [n]$ is a bijection. Define a new function $g : \mathbb{N} \to [n+1]$ by

$$g(m) = \begin{cases} f(m-1) & \text{if } m \geq 1 \\ n+1 & \text{if } m = 0 \end{cases}$$

It is easy to check that g is a bijection. This contradicts Theorem 8.31.

We also have:

Theorem 8.35. Subsets of finite sets are finite, supersets of infinite sets are infinite.

Proof. Exercise (assignment 6). □

8.2.2. *To infinity and beyond.* How does the notion of having the same cardinality match our intuition for infinite sets? We will see some very surprising facts happen. For a start, recall that $\mathbb{N} \subset \mathbb{Z}$ and $\mathbb{Z} \backslash \mathbb{N}$ is infinite. However:

Theorem 8.36. $\mathbb{N}$ and $\mathbb{Z}$ are equipotent: there is a bijection $f : \mathbb{N} \to \mathbb{Z}$.

Proof. Define

$$f(n) = \begin{cases} -\frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n+1}{2} & \text{if } n \text{ is odd} \end{cases}$$

(So the sequence of values $f(0), f(1), f(2), f(3), \ldots$ looks like $0, 1, -1, 2, -2, \ldots$).

f is an injection: if $f(n) = f(n')$, then clearly if n and n' are both even (or both odd), $n = n'$, so assume without loss of generality that n is even and n' is odd. Then we have $-\frac{n}{2} = \frac{n'+1}{2}$, so $-n = n' + 1$, so $0 = n' + n + 1$. Now n' and n are both natural numbers, so $n' + n + 1 > 0$, a contradiction.

f is a surjection: given $m \in \mathbb{Z}$, we consider two cases. Either $m > 0$, in which case $2m - 1 \in \mathbb{N}$ and $f(2m - 1) = m$, or $m \leq 0$, in which case $-2m \in \mathbb{N}$ and $f(-2m) = m$.

Therefore f is a bijection, as needed. □

This tells us that we can "rename" the natural numbers to make them into the integers. In other words, one can give a list of all the integers that looks like $a_0, a_1, a_2, \ldots$. We give this property a name:

Definition 8.37. A set is called *countable* if it is equipotent to $\mathbb{N}$. An infinite set that is not countable is called *uncountable*. A set is called *at most countable* if it is countable or finite.

So the previous result tells us that $\mathbb{Z}$ is countable. To show a set A is countable, we have to *exhibit* a bijection from $\mathbb{N}$ to A, or intuitively we have to show how to *list* A as $a_0, a_1, a_2, \ldots$ in such a way that the list contains no repetitions and that for every $a \in A$ there is $n \in \mathbb{N}$ such that $a_n = a$. Such a sequence is sometimes called an *enumeration*.

In a sense, the countable sets are the "smallest" possible infinite sets. We include the proofs of some of the next facts for reference, but they have not been discussed in class.

Fact 8.38. Assume A is an infinite subset of $\mathbb{N}$. Then A is countable.

Proof. We define a bijection $f : \mathbb{N} \to A$ *inductively* as follows:

- $f(0)$ is the minimal element of A (note that A is infinite, so non-empty).
- $f(n+1)$ is the minimal element of $A \backslash \{f(0), ..., f(n)\}$. Note that the latter set is non-empty, since we are assuming that A is infinite.

f is an injection: if $f(n) = f(m)$, assume by symmetry $n \leq m$. If $n < m$, then as $f(m)$ is an element of $A \backslash \{f(0), ..., f(n)\}$, $f(m) \neq f(n)$, so $n = m$.

f is a surjection: if not, let m be the minimal element of A that is not in the range of f (i.e. there is no $n \in \mathbb{N}$ such that $f(n) = m$). Then we must have $f(m) \geq m$, but the definition of f tells us that $f(m)$. Let k be minimal such that $f(k) \geq m$. Then by minimality of m we must have $f(k) = m$, a contradiction. □

By some "renaming", we can also prove:

Fact 8.39.

(1) A set A is countable if and only if A is infinite and there is an *injection* $f : A \to \mathbb{N}$.
(2) An infinite subset of a countable set is countable.

We then obtain:

Fact 8.40. If $f : \mathbb{N} \to A$ is a surjection, then A is at most countable. More generally, if B is countable and $f : B \to A$ is a surjection, then A is at most countable.

Proof. We prove the first part. The second follows by "renaming" B to $\mathbb{N}$ (exercise).

One can define $g : A \to \mathbb{N}$ by $g(a) =$ the minimal n such that $f(n) = a$. g is an injection: if $g(a) = g(a') = n$, then $f(n) = a = a'$. If A is finite, there is nothing to prove, and if A is infinite, we apply Fact 8.39.(1) to see that A is countable. □

Are there sets that are larger than countable? Now that we have seen that $\mathbb{Z}$ is countable, the next natural candidate would be $\mathbb{Q}$. It turns out it is also countable. First, we prove the following stronger result:

Theorem 8.41. $\mathbb{N} \times \mathbb{N}$ is countable.

Proof sketch. We list the pairs of natural numbers in the following way

$$(0,0),(0,1),(1,0),(2,0),(1,1),(0,2),(3,0),(2,1),(1,2),(3,0),\dots$$

Explicitly, there are only finitely many pairs whose components sum to 0, and list them first. Then we list the pairs whose components sum to 1, then those whose components sum to 2, and so on. This is injective, since we never repeat the same pair. This is surjective, since given a pair $(a,b) \in \mathbb{N} \times \mathbb{N}$, there are only finitely many pairs with sum $< n := a + b$, and only finitely many pairs with sum $\leq n$ before (a,b).

Although it can be done, it is a bit painful and no too insightful to explicitly write the bijection we obtain, so we will leave this as an exercise. □

Another more formal but less conceptual proof. We use problem 3 of assignment 5 to see that every positive natural number n can be uniquely written as $n = 2^m k$ for k, m natural numbers and k odd. In other words, n can be associated to the pair (m,k). We do not yet have our bijection, since k is required to be odd, and n positive, but we are very close. Define the function $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ by $f(n) = (m, \frac{k-1}{2})$, where k and m are such that $n + 1 = 2^m k$ and k is odd. We leave it as an exercise to see that f is a bijection. □

By some renaming left as an exercise (assignment 6), we obtain the more general:

Theorem 8.42. If A and B are countable, then $A \times B$ is countable.

Theorem 8.43. $\mathbb{Q}$ is countable.

Proof. By Theorem 8.36, $\mathbb{Z}$ is countable. By Theorem 8.42, $\mathbb{Z} \times \mathbb{Z}$ is countable. Now the map $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}$ given by $f(m,n) := \frac{m}{|n|+1}$ is a surjection (why?). Since it is a superset of $\mathbb{N}$, $\mathbb{Q}$ is infinite and we have just seen that $\mathbb{Z} \times \mathbb{Z}$ is countable. Therefore by Theorem 8.40, $\mathbb{Q}$ is countable. □

We can also obtain the following very handy result. While again not too hard, the proof has not been discussed in class.

Fact 8.44. Assume $\mathcal{F}$ is an at most countable family of at most countable sets, i.e. $\mathcal{F} = \{A_0, A_1, \dots\}$, where A_n is at most countable for each $n \in \mathbb{N}$. Then the union $\bigcup_{A \in \mathcal{F}} A = \bigcup_{n=0}^{\infty} A_n$ is at most countable.

Proof. For each $n \in \mathbb{N}$, we may assume by putting more elements inside A_n (e.g. by replacing A_n by $A_n \cup \mathbb{N}$) that A_n is countable. Let $A := \bigcup_{n=0}^{\infty} A_n$. Let $f : \mathbb{N} \times \mathbb{N} \to A$ be defined by $f(n,m) := f_n(m)$ (i.e. we pick the mth element from the nth set). Note that f need not

be injective, as there could be duplicate elements, but we claim that f is surjective: given $a \in A$, $a \in A_n$ for some n, and hence since f_n is surjective there exists m so that $f_n(m) = a$. Thus $f(n, m) = a$. This proves that f is surjective. By Fact 8.40, A is at most countable. $\square$

Now that we know $\mathbb{Q}$ is countable, it is natural to ask whether $\mathbb{R}$ is countable. It turns out this is not true: $\mathbb{R}$ is uncountable. We will need the following fact, whose proof uses the completeness axiom:

Fact 8.45. Every real number $0 < x < 1$ has a decimal expansion, i.e. there is a sequence $a_0, a_1, a_2, \ldots$ with $a_i \in \{0, ..., 9\}$ such that $x = 0.a_0a_1a_2\ldots$[16]. In general, this sequence is not unique, i.e. there could be two sequences describing the same number (like $0.1000000\ldots = 0.099999\ldots$). However, two distinct sequences which do not contain any 9 describe distinct real numbers.

Here, lecture 13 ended and lecture 14 started

We are now ready to prove uncountability of the reals. The method of proof is called *diagonalization* and is due to Cantor:

Theorem 8.46. $\mathbb{R}$ is uncountable.

Proof. $\mathbb{R}$ is infinite, so it is enough to see it is not countable. Assume for a contradiction that it is. Then any infinite subset of it is also countable. In particular, the set X of real numbers $0 < x < 1$ which have a decimal expansion containing only 0s and 1s is countable. Let $f : \mathbb{N} \to X$ be a bijection. Write a_i instead of $f(i)$. Then we have a list of all the elements of X containing no repetitions: $a_0, a_1, a_2, \ldots$. Each a_i has a decimal expansion $a_{i,0}, a_{i,1}, a_{i,2}, \ldots$ with $a_{i,j} \in \{0, 1\}$ for all i and j. Here is a table of the elements of X and their decimal expansion:

$$
\begin{aligned}
&0.a_{0,0}a_{0,1}a_{0,2}a_{0,3}a_{0,4}\ldots\\
&0.a_{1,0}a_{1,1}a_{1,2}a_{1,3}a_{1,4}\ldots\\
&\ldots\\
&0.a_{i,0}a_{i,1}a_{i,2}a_{i,3}a_{i,4}\ldots a_{i,i}\ldots\\
&\ldots
\end{aligned}
$$

From this table, we build a new member of X: For i a natural number, we let b_i be $1 - a_{i,i}$, i.e. it is 0 if $a_{i,i}$ is 1, and 1 if $a_{i,i}$ is

[16]We have not defined what this means exactly, but you can just think of it as saying that from the sequence one can reconstitute the number (this actually means $x = \sum_{i=0}^{\infty} a_i 10^{-(i+1)}$, but we will not discuss infinite sums in this course).

0. Let $x := 0.b_0b_1b_2\ldots$. Intuitively, the decimals of x are built by going through the diagonal of the table and taking the opposite of each number there. Then $x \in X$ since its decimal expansion contains only zeroes and ones. Since f is surjective, there is a natural number i such that $a_i = x$, and so by uniqueness of decimal expansions containing no 9s, we must have $a_{i,j} = b_j$ for all natural numbers j. In particular, $a_{i,i} = b_i$, but this is impossible since we defined b_i to be $1 - a_{i,i}$. We arrived at a contradiction, and this means X (and therefore $\mathbb{R}$) is not countable. □

From this result, we can conclude that in a well-defined sense, $\mathbb{R}$ has *many* more elements than $\mathbb{N}$: there are infinitely many reals and infinitely many natural numbers, but the infinity of reals is strictly bigger than the infinity of natural numbers! This has many consequences, some of which you will explore in your homework. For example, we can deduce that there are uncountably many irrational numbers, or that there are problems no computer program will ever be able to solve. Using a similar method, one can also show that there is no largest size of infinity: for every set A, there is a set B that is "strictly bigger" than A, in the sense that there is no surjection from A to B.

End of lecture 14

9. Combinatorics

9.1. **Counting.** *Lecture 15 started here.*

We now go back to sizes of finite sets, and become interested in computing them exactly in order to solve very concrete problems. Examples include computing the probabilities of various poker hands, the number of solutions to integer equations, and the number of possible paths between two points on a grid.

Most of the counting problems we will see are at the bottom solved using two amazingly useful principles: the rule of sum and the rule of product:

Theorem 9.1 (The rule of sum)**.** If A and B are two disjoint (i.e. $A \cap B = \emptyset$) finite sets, then $|A \cup B| = |A| + |B|$. More generally, if $n \in \mathbb{N}$ and $A_0, A_1, \ldots, A_n$ are *pairwise disjoint* finite sets, then:

$$|A_0 \cup A_1 \cup \ldots \cup A_n| = \sum_{i=0}^{n} |A_i| = |A_0| + |A_1| + \ldots + |A_n|$$

By "$A_0, A_1, \ldots, A_n$ are pairwise disjoint", we mean that any two of them are disjoint, i.e. for any distinct i and j, $A_i \cap A_j = \emptyset$. You will

prove the rule of sum for two sets in assignment 7. Let's see how we can prove the general version from the two sets version:

Proof of the general rule of sum from the rule of sum for two sets. We use induction on n. For the base case, if $n = 0$, there is only one set and the rule of sum just tells us $|A_0| = |A_0|$, which is true. For the inductive step, assume the rule of sum is true for n sets, and let's prove it for $n + 1$ pairwise disjoint finite sets $A_0, A_1, \ldots, A_{n+1}$. Let $A := A_0 \cup A_1 \cup \ldots \cup A_n$, and let $B := A_{n+1}$. We want to compute the size of $A_0 \cup A_1 \cup \ldots \cup A_{n+1} = A \cup B$. Also, the induction hypothesis tells us $|A| = \sum_{i=0}^{n} |A_i|$. Moreover, we have that A and B are disjoint (if $x \in A \cap B$, then $x \in A_i \cap A_{n+1}$ for some $i \leq n$, which is impossible since the pairwise disjointness hypothesis tells us $A_i \cap A_{n+1} = \emptyset$). Thus we can apply the rule of sum for two sets to get that

$$|A_0 \cup A_1 \cup \ldots \cup A_{n+1}| = |A \cup B| = |A| + |B| = \left(\sum_{i=0}^{n} |A_i| \right) + |A_{n+1}| = \sum_{i=0}^{n+1} |A_i|$$

□

The rule of sum also has a more intuitive formulation:

Fact 9.2 (The rule of sum, version 2)**.** Let C be a finite set. If we know each element of C is of *exactly one* type among $T_0, T_1, \ldots, T_n$, and there are c_i many elements of type i, then $|C| = \sum_{i=0}^{n} c_i$.

Example 9.3. Let's say we would like to compute how many natural numbers less than 100 are divisible by either 2 or 3. Let A be the set of natural numbers less than 100 divisible by 2, and let B be the set of natural numbers less than 100 divisible by 3. We want to compute the size of $A \cup B$. The members of A are $0, 2, \ldots, 98$, and there are $\frac{98}{2} + 1 = 50$ of them. Similarly, B contains $\frac{99}{3} + 1 = 34$ numbers. Does this mean that by the rule of sum, $|A \cup B| = |A| + |B| = 50 + 34 = 84$? *No*, since some numbers like 0 and 6 are both divisible by 2 and 3, and so it is not true that A and B are disjoint, or said another way using the "version 2" formulation of the rule of sum, it is not true that each number between 0 and 100 is of exactly one type. It turns out that $A \cap B$ contains exactly the multiples of 6 (this is not that easy to prove, but it follows from uniqueness of prime factorization and you can take it as granted for now), and that there are exactly $\frac{96}{6} + 1 = 17$ of them. When computing $|A| + |B|$, we are basically adding the multiples of 6 twice, so to get the right size of $A \cup B$, we must substract them once: $|A \cup B| = |A| + |B| - |A \cap B| = 50 + 34 - 17 = 67$.

The rule we just used to compute $A \cup B$ when they are not necessarily disjoint holds in general. Note that if A and B are disjoint, $|A \cap B| = |\emptyset| = 0$ and we recover the rule of sum.

Theorem 9.4 (The inclusion-exclusion principle)**.** For any finite sets A and B, $|A \cup B| = |A| + |B| - |A \cap B|$.

Proof. Assignment 7. □

Remark 9.5. There is also a more general version to compute $|A_0 \cup A_1 \cup \ldots \cup A_n|$, but we will not see it in this class. You might want to think about what form it would take.

To state the rule of product, we first formally define a notation for products of more than two numbers:

Definition 9.6 (Π notation)**.** Assume $f : (\mathbb{N} \backslash \{0\}) \to \mathbb{R}$ is a function and n is a natural number. We define $\prod_{i=1}^{n} f(i)$ inductively as follows:

- $\prod_{i=1}^{n} f(i) = 1$ if $n = 0$.
- $\prod_{i=1}^{n+1} f(i) = f(n+1) \cdot \prod_{i=1}^{n} f(i)$.

We can similarly define $\prod_{i=k}^{n} f(i)$ for k a natural number. If $k > n$, we adopt the convention that this is one.

Fact 9.7 (The rule of product)**.** For any two finite sets A and B, $|A \times B| = |A| \cdot |B|$. More generally, if $n \in \mathbb{N}$ and $A_0, A_1, \ldots A_n$ are finite sets, then:

$$|A_0 \times A_1 \times \ldots \times A_n| = \prod_{i=0}^{n} |A_i| = |A_0| \cdot |A_1| \cdot \ldots \cdot |A_n|$$

Remark 9.8. In general, for three sets A, B, C, $(A \times B) \times C \neq A \times (B \times C)$ (the elements of the first are of the form $((a, b), c)$, the elements of the second are of the form $(a, (b, c))$. This difference is almost never of importance, and we will adopt the convention that cartesian products are computed by putting the brackets on the left, i.e. $A \times B \times C = (A \times B) \times C$. We will write (a, b, c) instead of $((a, b), c)$, and similarly for longer products.

Similarly to the way we proved the general rule of sum from the two sets version, we can prove the general rule of product from the rule of product for two sets. The latter can be proven using induction and the rule of sum, but this is a somewhat slow-going proof that we will not discuss. It's an excellent exercise for you to try!

The rule of product also has a more intuitive formulation:

Fact 9.9 (The rule of product, version 2)**.** Let C be a finite set. If each element of C can be described in a unique way using a procedure involving $n+1$ steps $S_0, S_1, \ldots, S_n$, and each step S_i can be performed in c_i ways *regardless of how* $S_0, S_1, \ldots, S_{i-1}$ *are performed*, then $|C| = \prod_{i=0}^{n} c_i$.

Example 9.10. Recall from assignment 6 that for n a natural number, a *binary n-tuple* is a function from $[n]$ to $\{0, 1\}$, which you can think of as a string of n bits (0s or 1s). Fix a natural number n, and let C be the set of binary n-tuples. We can think of building a binary tuple as a procedure consisting in n steps $S_1, \ldots, S_n$, where at the ith step we choose whether the ith coordinate of the tuple is 0 or 1. This choice does not depend on the previous steps, and there are two ways of making it, therefore by the rule of product there are $\prod_{i=1}^{n} 2 = 2^n$ many ways of choosing a binary n-tuple, and therefore there are 2^n many binary n-tuples: $|C| = 2^n$.

Remembering assignment 6, there is a bijection from $\mathcal{P}([n])$ to the set of binary n-tuples, and hence $|\mathcal{P}([n])| = 2^n$. More generally, for a finite set A, $|\mathcal{P}(A)| = 2^{|A|}$. If you have not found this argument convincing enough, we give another proof of this result using induction and the rule of sum:

Theorem 9.11. For any finite set A, $|\mathcal{P}(A)| = 2^{|A|}$.

Proof. Let $n := |A|$. We use induction on n. For the base case, if $n = 0$, then $A = \emptyset$, and $|\mathcal{P}(\emptyset)| = |\{\emptyset\}| = 1 = 2^0$. For the inductive step, assume the result is true for all sets of size n, and assume $|A| = n + 1$. In particular, $|A| \geq 1$, so A is non-empty. Fix $a \in A$. We can partition $\mathcal{P}(A)$ into the set X of subsets of A that do not contain a and the set Y of subsets of A that do contain a. We have that $X \cap Y = \emptyset$ and $\mathcal{P}(A) = X \cup Y$. Moreover, if we let $A' := A \backslash \{a\}$, we have that:

(1) $|A'| = n$, and hence by the inductive hypothesis $|\mathcal{P}(A')| = 2^n$.
(2) $\mathcal{P}(A') = X$.
(3) There is a bijection[17] $f : X \to Y$ given by $f(S) = S \cup \{a\}$, and therefore $|Y| = |X| = 2^n$.

Thus by the rule of sum:

$$|\mathcal{P}(A)| = |X \cup Y| = |X| + |Y| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1} = 2^{|A|}$$

as needed. □

[17]We leave it to the reader to check it is really a bijection.

Remark 9.12. In the rule of product, it is important that the elements can be described in a unique way: consider the following wrong arguments to count the number of elements in the set $C := \{1, 2, 3, 4, 6\}$: every number can be built by first choosing a number k from 1 to 3, then choosing a number m from 1 to 2, and multiplying m and k together. Therefore $|C| = 3 \cdot 2 = 6$ (?!). While it is true that every number in C can be represented in the way described above, we are effectively counting $2 \cdot 3$ and $3 \cdot 2$ as a different number...

Here, lecture 15 ended and lecture 16 started.

Example 9.13. Five planes need to land at an airport one after the other. How many possible orderings are there? To figure this out, number the plane from 1 to 5 and the possible landing positions from 1 to 5 (the plane in position 1 lands first). To describe a possible landing order, we can think of plane 1 choosing one landing position between 1 and 5 (five choices), then plane 2 choosing one of the renaming choices (four of them), and so on until plane 5 takes the only leftover spot. The choices at each step depend on the choices made at the preceeding ones, but the *number* of those choices doesn't. Therefore by the rule of product there are $5 \cdot 4 \cdot \ldots \cdot 1 = 120$ possible orderings.

In the example above, a landing order can be seen as a function mapping plane i to its landing position. Such a function will be a bijection (no position will be empty, and two distinct planes get two distinct positions). We give such a map a name:

Definition 9.14. For any set A, a bijection from A to A is called a *permutation* of A.

Generalizing the previous example, we obtain:

Theorem 9.15. For n a natural number, $[n]$ (or any set with n elements) has exactly $\prod_{i=1}^{n} i$ permutations.

Note that this works even if $n = 0$, since there is exactly one permutation (the empty function) from the empty set to itself.

Notation 9.16. For n a natural number, denote by $n!$ (said "n factorial") the number $\prod_{i=1}^{n} i$. Alternatively, $n!$ can be defined inductively to be 1 if $n = 0$ or $(n-1)! \cdot n$ for $n \geq 1$.

So a reformulation of the previous theorem is that for any natural number n, there are $n!$ permutations of $[n]$. More generally, we can ask for the number of ways to arrange any k distinct elements of $[n]$ into a list (so order matters and repetitions are not allowed). Such

lists are sometimes called *arrangements*. Notice that this is the same as counting the number of injections from $[k]$ to $[n]$.

Theorem 9.17. For natural numbers $k \leq n$, the number of arrangements of k distinct elements of $[n]$ is given by:

$$n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \prod_{i=0}^{k-1}(n-i) = \frac{n!}{(n-k)!}$$

Proof. We can build an arrangement of k elements by first selecting the first element out of the n available ones, then select the second element out of the $(n-1)$ remaining choices, and continuing this way until there are $(n-k+1)$ possible choices for the kth element. From the rule of product, we obtain the result. □

Note that this agrees with the formula for the number of permutations, where $k = n$.

Example 9.18. For $k = 2$ and $n = 3$, the 2-elements arrangements of [3] are 12,21,13,31,23,32 . There are $6 = \frac{3!}{(3-2)!}$ of them.

What if we ask for the number of ways to list k distinct elements of $[n]$ without repetitions when order does *not* matter? Such a list is just a k-elements subset of $[n]$, sometimes called a selection. We give the number of selections a name:

Definition 9.19 (Binomial coefficient)**.** The number of k-elements subset of $[n]$ is denoted by $\binom{n}{k}$ (said "n choose k").

If $k < 0$ or $k > n$, $\binom{n}{k}$ is 0 (there are no set with a negative number of elements, and no subset of $[n]$ has more than n elements), and if $0 \leq k \leq n$, there is a simple formula to compute it:

Theorem 9.20. If $0 \leq k \leq n$, then:

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

Proof. We count the number r of arrangements of k elements of $[n]$ in two ways: First, we have already seen that $r = \frac{n!}{(n-k)!}$. Second, to build an arrangements, one can first pick a k-element subset of $[n]$, and then order it in one of $k!$ possible ways. In this case the rule of product gives us $r = k!\binom{n}{k}$. Thus $\frac{n!}{(n-k)!} = k!\binom{n}{k}$. Divide by $k!$ to conclude. □

Example 9.21 (Number of poker hands)**.** Poker is a game played with a deck of 52 cards. Each card has a *rank* (one of $2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K, A$)

and a *suit* (one of spade, heart, club, diamond). A *hand* is a set of five (distinct) cards. Hands are ranked according to how rare they are: the smaller the number of possibilities for a hand to occur, the more valuable. Some specific hands are given names:

- A pair: two cards with the same rank.
- A three of a kind: three cards with the same rank.
- Four of a kind: Four cards with the same rank.
- A straight: The five cards can be listed to have consecutive ranks. The rank can start with 2, 3, ..., 10, or A (there are 10 possibilities)
- A flush: The five cards have the same suit.

Unless stated otherwise, hands such as three of a kind are also pairs. This differs from the standard poker terminology.

There are $\binom{52}{5} = 2598960$ possible hands, and there are for example $10 \cdot 4^5 = 10240$ possible straights (including straight flushes): there are 10 ways of picking up the starting rank, then 4 ways of picking up the suit for each of the 5 cards. There are $\binom{4}{1}\binom{13}{5} = 5148$ flushes: we first choose a suit, then choose five possible (necessarily distinct) ranks. Thus flushes occur less often and so are more valuable than straights. To compute the number of straight flushes, we note that a straight flush is entirely determined by the suit and the starting rank, so there are only $4 \cdot 10 = 40$ straight flushes. Thus the number of straights that are not straight flushes is $10 \cdot 4^5 - 40 = 10200$.

Assuming each hand is equally likely, the *probability* that a type of hand occurs is simply the number of possible hands with that type divided by the total number of hands. For example, the probability to obtain a straight flush is $\frac{40}{2598960}$ which is less than one in ten thousand. The probability to obtain a straight (or a straight flush) is $\frac{10240}{2598960} \approx 0.004$, or 4 in a thousand.

Remark 9.22. A *wrong* way to count the number of flushes would be to say that a flush can be described by first choosing one of 52 cards, then choosing the four remaining cards out of the 12 that have the suit of the first one, and finally concluding from the rule of product that there are $52 \cdot \binom{12}{4} = 25740$ flushes. The problem is that the description above is not unique: for example one could first choose an ace of spades, then a 2, 3, 5, 7, or one could first choose a 7 of spade and then an ace, 2, 3, 5.

The binomial coefficients appear in many areas of mathematics and have a number of very nice properties. For example:

Theorem 9.23 (Pascal's formula)**.** For any natural numbers k and n:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Proof. We give two types of proofs: a combinatorial proof that computes the same number in two different ways, and an algebraic proof that simply uses known formulas for the binomial coefficient. The algebraic proof is more formal, but also less insightful and technically harder to understand. The combinatorial proof gives information as to *why* the result is true, which is often something you expect of good proofs.

Combinatorial proof. We can choose a k-elements subset of $[n]$ by either excluding n and choosing k elements of $[n-1]$ ($\binom{n-1}{k}$ possibilities), or deciding to include n and choosing the $k-1$ remaining elements from $[n-1]$ ($\binom{n-1}{k-1}$ possibilities). Any k-elements subset is of exactly one of these two types, so by the rule of sum, the result follows.

Algebraic proof. The formula is true if $k > n$ (as all the coefficients involved are 0), and also if $k = n$ (both sides are 1, even if $k = n = 0$), so we may assume $k < n$ and $n > 0$. Note also that for $k = 0$, the formula holds (both sides are 1: $\binom{n}{0} = 1$ for any integer n). Thus we can assume $1 \leq k < n$. We did this checking to make sure that $(n-1-k)!$, $(k-1)!$, or $(n-1)!$ made sense (recall that we haven't defined what we meant by objects such as $(-1)!$). Now let's compute:

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-1-k)!} \\
&= \frac{k(n-1)!}{k!(n-k)!} + \frac{(n-k)(n-1)!}{k!(n-k)!} \\
&= \frac{k(n-1)! + (n-k)(n-1)!}{k!(n-k)!} \\
&= \frac{n(n-1)!}{k!(n-k)!} \\
&= \frac{n!}{k!(n-k)!} \\
&= \binom{n}{k}
\end{aligned}$$

□

Thus we can generate the binomial coefficients inductively by building *Pascal's triangle*: its rows are numbered starting from 0: row n contains $n+1$ elements, and the first and last element of row n are

always 1 (they denote $\binom{n}{0}$ and $\binom{n}{n}$ respectively). Elements of each row are numbered from 0 to n. To compute element number k of row n, for $1 \leq k < n$, add elements $k-1$ and k of row $n-1$ together. By Pascal's formula, it follows that element k of row n is exactly $\binom{n}{k}$. The first few rows of Pascal's triangle are:

```
            1
          1   1
        1   2   1
      1   3   3   1
    1   4   6   4   1
  1   5   10  10  5   1
```

From this we can for example read off that $\binom{5}{2} = 10$.

An interesting open problem regarding Pascal's triangle is *Singmaster's conjecture*: There a natural number N such that every number larger than one appears at most N times in Pascal's triangle. As of 2014, it is unknown whether any number larger than one can appear more than 8 times in Pascal's triangle (the only number known to appear 8 times is 3003). There are no known examples of numbers appearing exactly five or exactly seven times.

Here, lecture 16 ended and lecture 17 started (algebraic proof of Pascal's formula covered in lecture 17).

The binomial coefficients also appear in a formula for powers of sums:

Theorem 9.24 (The binomial theorem)**.** For any real numbers x and y and any natural number n:

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

Before proving it, we need some simple facts about sums:

Theorem 9.25. For $f, g : \mathbb{N} \to \mathbb{R}$, n a natural number, and c a real number:

(1) $\sum_{i=0}^{n} cf(i) = c \sum_{i=1}^{n} f(i)$.
(2) $\sum_{i=0}^{n} f(i) + g(i) = (\sum_{i=0}^{n} f(i)) + (\sum_{i=0}^{n} g(i))$.

Proof. Exercise: use induction. □

Proof of the binomial theorem. Again, we can prove this both algebraically or combinatorially.

Combinatorial proof. We can see the identity is true by observing that the coefficient of $x^k y^{n-k}$ in the expansion of $(x+y)^n$ is going to be the number of ways to choose x k times out of n when applying the

distributive law and choosing y the other times. A little bit of thinking should convince you that this is $\binom{n}{k}$.

Algebraic proof. We prove the identity by induction on n. If $n = 0$, then both the left hand side and right hand side are one. Now assume the result is true for n and let's prove it for $n+1$. Using the induction hypothesis, expand:

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n \\
&= (x+y)\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k}x^{k+1}y^{n-k} + \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k+1} \\
&= \sum_{k=1}^{n+1}\binom{n}{k-1}x^k y^{n-k+1} + \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k+1} \\
&= x^{n+1} + y^{n+1} + \sum_{k=1}^{n}\binom{n}{k-1}x^k y^{n-k+1} + \sum_{k=1}^{n}\binom{n}{k}x^k y^{n-k+1} \\
&= x^{n+1} + y^{n+1} + \sum_{k=1}^{n}\left(\binom{n}{k-1} + \binom{n}{k}\right)x^k y^{n+1-k} \\
&= x^{n+1} + y^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}x^k y^{n+1-k} \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}x^k y^{n+1-k}
\end{aligned}$$

You should be able to follow each step. We first make a change of variable and rearrange the sums in order to be able to use Theorem 9.23. Once this theorem has been used, we put the sums back together. □

Example 9.26. Using the binomial theorem, we can compute

$$(x+y)^4 = \sum_{i=0}^{4}\binom{4}{k}x^k y^{n-k} = y^4 + 4y^3x + 6y^2x^2 + 4x^3y + x^4$$

Where we have used that $\binom{4}{1} = \binom{4}{3} = 4$ and $\binom{4}{2} = 6$.

So far, we have given formulas for the number of ways to select $k \leq n$ elements of $[n]$ when repetitions are allowed and order matters (this is n^k, by a straightforward generalization of Example 9.10), when

repetitions are not allowed and order does not matter (this is $\binom{n}{k}$), and when repetitions are not allowed and order does matter (this is $\frac{n!}{(n-k)!}$). We now investigate the remaining case.

Theorem 9.27. For k and n natural numbers, $n \geq 1$, the number of ways to pick k elements of $[n]$ when you are allowed to repeat the same element and order does not matter is $\binom{k+n-1}{n-1}$. This is also the number of natural number solutions to the equation $x_1 + x_2 + \ldots + x_n = k$.

Proof. For the last sentence, simply observe that a list of k elements where order does not matter but elements can be repeated can be completely described by giving for each $i \in [n]$ the number of times (x_i) it appears in the list. Since the list has k elements, we must have $x_1 + x_2 + \ldots + x_n = k$.

To compute the number of solutions to such an equation, we think of having k units to allocate between $x_1, \ldots, x_n$: we think of our k units as k dots on a line (think of writing k in "base 1"), that have to be separated by $n-1$ "+"s. For example, if $n = 4$ and $k = 8$, the solution $x_1 = 1$, $x_2 = 0$, $x_3 = 4$, and $x_4 = 3$ would be described by:

$$\cdot + + \cdot \cdot \cdot \cdot + \cdot \cdot \cdot$$

Thus all we have to do is decide where to put the $n-1$ "+"s. There are $k + n - 1$ many possible positions and $n - 1$ many "+"s, so the total number of solutions is $\binom{k+n-1}{n-1}$. □

Remark 9.28. As often with those kind of combinatorial arguments, it is safer to try to remember the proof than to try to remember the final formula.

To sum up, we have derived the following formulas to compute the number of ways to pick k out of n elements (where $k, n \in \mathbb{N}$):

	With repetitions	Without repetitions
Ordered	n^k	$\frac{n!}{(n-k)!}$ if $k \leq n$, 0 otherwise
Unordered	$\binom{k+n-1}{n-1}$ if $k \geq 1$, 1 otherwise	$\binom{n}{k}$

Here, lecture 17 ended, and lecture 18 started.

9.2. **The pigeonhole principle.** The simplest application of the pigeonhole principle (often attributed to Daniel Kleitman) is that out of three people (with a well-determined sex), two must have the same sex. More generally:

Theorem 9.29. For k and n natural numbers, if we place more than kn objects into n boxes, then one box must have more than k elements.

Said more formally, if $m > kn$, and $f : [m] \to [n]$, then for some $i \in [n]$, $|f^{-1}[\{i\}]| > k$.

Proof. We have that $f^{-1}[[n]] = [m]$ (f maps any element of $[m]$ somewhere in $[n]$), and for any two distinct i and j in $[n]$, $f^{-1}[\{i\}] \cap f^{-1}[\{j\}] = \emptyset$ (an element of $[m]$ cannot be sent both to i and to j). Thus using the rule of sum with $A_i := f^{-1}[\{i\}]$:

$$m = |f^{-1}[[n]]| = \sum_{i=1}^{n} |A_i|$$

Now assume for a contradiction that $|A_i| \leq k$ for all i. Then $m = \sum_{i=1}^{n} |A_i| \leq \sum_{i=1}^{n} k = nk$, which contradicts the hypothesis that $m > nk$. □

Although it is very intuitive and simple to prove, the pigeonhole principle can be used to demonstrate many non-obvious facts. The name comes from the fun obvious fact that if we take more than n pigeons and put them into n boxes, then one box must contain more than one pigeon (this is an application of the principle with $k = 1$).

Example 9.30. In Pittsburgh, two people must have the exact same number of hairs: It is estimated than an average human head has about $n := 150000$ hairs, and Pittsburgh has about $m := 300000$ inhabitants (it has more, but let's take away the inhabitants that have more than 150000 hairs from that number). If we take the people of Pittsburgh to be the objects and the number of hairs to be the box of an object in the pigeonhole principle, we obtain that two objects must fall into the same box, i.e. two inhabitants of Pittsburgh must have the same number of hairs. Note that the proof is *nonconstructive*: it tells us nothing about who those people are. This comes from the fact the pigeonhole principle was proven by contradiction.

The pigeonhole principle was introduced by Dirichlet in 1834 in order to study approximation of real numbers with rationals. To motivate the next result, assume you want to approximate π with a rational number (it is a nontrivial fact that π is irrational). Assume you want your rational number to have a denominator less than or equal 100. You might think that $\frac{314}{100}$ would then be a reasonable approximation, but actually a bigger denominator is not always better: $\frac{22}{7}$ is a slightly better approximation to π, and $\frac{333}{106}$ is correct to four decimal places. More generally, you may ask how close an approximation you can achieve if you want your denominator to have size less than n. This is the question Dirichlet's result answers:

Theorem 9.31 (Dirichlet's approximation theorem)**.** For every real number x and positive natural number n, there exists a rational $\frac{p}{q}$ with p, q integers, $1 \leq q \leq n$ and:

$$\left| x - \frac{p}{q} \right| < \frac{1}{qn} \leq \frac{1}{q^2}$$

This tells us in particular that real numbers can be approximated arbitrarily closely by rational numbers. Before presenting the proof, we need one more fact about the real numbers. The proof uses the completeness axiom.

Fact 9.32. For every real number x, there is a unique integer n such that $n \leq x < n + 1$.

Definition 9.33. For x and n as above, we call n the *floor* of x and write $n = \lfloor x \rfloor$. If x is not an integer, we call $n + 1$ the *ceiling* of x and write $n + 1 = \lceil x \rceil$. If x is an integer, its ceiling is just x. The *fractional part* $\langle x \rangle$ of x is defined to be $x - \lfloor x \rfloor$.

Example 9.34. The fractional part of 1 is 0, and its ceiling and floor are 1. The ceiling of $\frac{4}{3}$ is 2, its floor is 1, and its fractional part is $\frac{1}{3}$. The fractional part of π is $\pi - 3 = 0.1415\ldots$. Its floor is 3 and its ceiling is 4.

Proof of Dirichlet's approximation theorem. Let x be a real number and n a positive natural number. Consider the fractional parts:

$$\langle 0 \rangle, \langle x \rangle, \langle 2x \rangle, \ldots, \langle nx \rangle$$

They form $n + 1$ numbers and each falls into exactly one of the intervals:

$$\left[0, \frac{1}{n}\right), \left[\frac{1}{n}, \frac{2}{n}\right), \ldots, \left[\frac{n-1}{n}, 1\right)$$

There are only n such intervals. Therefore[18] by the pigeonhole principle there exists $i < j$ in $\{0\} \cup [n]$ such that $\langle ix \rangle$ and $\langle jx \rangle$ fall into the same interval. In particular, $|\langle jx \rangle - \langle ix \rangle| < \frac{1}{n}$. This implies[19] that $x(j - i)$ is at distance less than $\frac{1}{n}$ from an integer, i.e. for some integer p, $|x(j-i) - p| < \frac{1}{n}$. Let $q := j - i$. Then we have $|qx - p| < \frac{1}{n}$. Dividing

[18]It could actually be that for some $i \neq j$, $\langle xi \rangle = \langle xj \rangle$. In this case the pigeonhole principle does not apply but we also get that they are in the same interval.

[19]Exercise 1 in the additional problems for week 4 asks you to check this formally. This is not a very hard fact to believe though: think of the decimal representation of real numbers.

the inequality by q, $|x - \frac{p}{q}| < \frac{1}{nq}$. We also have $\frac{1}{nq} \leq \frac{1}{q^2}$ because we took $q \leq n$. □

Another simple application of the pigeonhole principle is:

Theorem 9.35. At a party with six students, there are three people that either all know each other, or all do not know each other (compare with problem 5 of assignment 3). We assume knowledge is a symmetric (but not necessarily transitive) relation.

Proof. Name the students $x_1, \ldots, x_6$. Look at the relationships x_1 can have with the five other students: for each $2 \leq i \leq 6$, either x_1 knows x_i or x_1 does not know x_i. We can see this as assigning each of these $m = 5$ students one of $n = 2$ boxes. By the pigeonhole principle, there are three students who either all know x_1, or all do not know x_1. By symmetry, we can assume we fall into the first case, and rearranging the names we can assume x_2, x_3, x_4 all know x_1. If any two of x_2, x_3, x_4 know each other, then as they also know x_1 we have found three students who all know each other. If none of x_2, x_3, x_4 know each other, then we have found three students who all do not know each other. □

If only five students are at the party, the result is no longer true (can you think of an example?). Questions asking for the largest (or smallest) object with a given property are called *extremal problems*, and the pigeonhole principle is often extremely useful to solve them. Here is another extremal result:

Theorem 9.36 (The Erdős–Szekeres theorem)**.** Assume n is a natural number. Any sequence of n^2+1 distinct real numbers contains a monotone (i.e. either strictly increasing or strictly decreasing) subsequence of length $n + 1$.

Example 9.37. Take $n = 2$. The sequence $1, 3, -1, 0, -\pi$ has length $5 = 2^2 + 1$, and so according to the theorem must contain a monotone subsequence of length 3. Indeed, $1, 0, -\pi$ is such a subsequence. By inspection, it can be seen that the first four elements do not contain a monotone subsequence of length 3. In general, $n^2 + 1$ is the optimal length: for any natural n, there is a sequence of length n^2 with no monotone subsequence of length n (can you see why?).

Proof of the Erdős–Szekeres theorem. Let $a_1, a_2, \ldots a_{n^2+1}$ be an arbitrary sequence of distinct real numbers. For each $i \in [n^2 + 1]$, let x_i denote the length of the longest increasing subsequence *ending* at a_i, and let y_i denote the length of the longest decreasing subsequence ending at a_i (so in the example above, $x_4 = 2$, as witnessed by the subsequence $-1, 0$). Assume for a contradiction the theorem fails. Then

$x_i, y_i \leq n$ for all $i \in [n^2 + 1]$. Since we also have that $x_i, y_i \geq 1$ for all i, we have $x_i, y_i \in [n]$, so for a fixed i, the product rule tells us that the number of possible pairs (x_i, y_i) is $|[n] \times [n]| = n^2$. Now there are $n^2 + 1$ many possible is, and only n^2 possible values for the pairs, thus the pigeonhole principle tells us there must exist $i < j$ such that $(x_i, y_i) = (x_j, y_j)$. There are two cases: either $a_i < a_j$ or $a_i > a_j$. If $a_i < a_j$, then it cannot be that $x_i = x_j$, as any increasing subsequence ending with a_i induces an increasing subsequence ending with a_j with one more element. Similarly, if $a_i > a_j$, $y_i \neq y_j$. This contradiction concludes the proof. □

Here, lecture 18 ended, and lecture 19 started.

10. Number theory

Number theory is one of the oldest classical areas of mathematics, where there are many beautiful results and many open questions (such as Goldbach's conjecture). We will also present an application to communicating securely on the internet. For now, we just mention the problem we will discuss: assume Alice and Bob want to privately communicate over the internet, but their communications are monitored. How can they hide the content of their messages?

10.1. **The fundamental theorem of arithmetic.** After an earlier introduction to prime numbers, culminating in Theorem 7.18, we now begin a more systematic study. Recall the following facts about dividing and being coprime:

Theorem 10.1. Assume n, m, and k are integers.

(1) If k divides n and k divides m, then k divides $n + m$.
(2) If k divides n, then k divides $n \cdot m$.
(3) If m and n are coprime, then n and $m - n$ are coprime.

Proof. These were covered in assignment 5 (the last fact was mistated there but is still correct by the same proof). For completeness, we give the proofs:

(1) Fix $n' \in \mathbb{Z}$ such that $n = kn'$. Fix $m' \in \mathbb{Z}$ such that $m = km'$. Then $n + m = k(n' + m')$ so k divides $m + n$.
(2) Fix n' such that $n = kn'$. Then $nm = kn'm = k(n'm)$ so k divides $n \cdot m$.
(3) Assume m and n are coprime but n and $m - n$ are not. Then there exists a prime p dividing n and $m - n$. By (1), p divides $n + m - n = m$. Thus p divides m and n and so m and n are not coprime, contradiction.

□

Recall that a natural number $n \geq 2$ is prime if the only natural numbers dividing it are 1 and n. The first few primes are $2, 3, 5, 7, 11, 13, \ldots$. Now, it is far from obvious that this list goes on forever. From what we know so far, it could be that there are only a billion primes, and that all numbers are a product of those. It turns out this is not the case. This was shown by Euclid already around 300 BC.

Theorem 10.2. There are infinitely many primes.

Proof. Assume $n \in \mathbb{N}$ and $p_0, p_1, \ldots, p_n$ are distinct prime numbers. We build a new prime q which is not in this list, showing that there must be more than $n+1$ primes. Since n is arbitrary, the result will follow.

Consider $m := p_0 p_1 \ldots p_n + 1$. m is *not* necessarily prime[20], but by Theorem 7.18 there must be a prime q that divides m. Thus q cannot divide $m - 1 = p_0 p_1 \ldots p_n$ (if q divides $m-1$ then as q also divides m, Theorem 10.1 tells us that q divides $m - (m-1) = 1$, which is impossible as q is prime), so q cannot be one of $p_0, \ldots, p_n$. □

Our next goal is to prove uniqueness of a number's prime factorization. This turns out to be surprisingly tricky. A *very* useful fundamental result toward this goal is:

Theorem 10.3 (Bézout's lemma)**.** Assume m and n are coprime integers. Then there exists integers a and b such that $am + bn = 1$.

Proof. We can assume that m and n are natural numbers: once the result is proven for the natural numbers, we can replace m and n by $-m$ and $-n$ if necessary and correspondingly change the signs of the a and b we obtain.

We prove the result by strong induction on $m+n$, i.e. we prove $p(x)$ by strong induction where $p(x)$ says: for every natural numbers n and m such that $x = m + n$, if n and m are coprime, there exists integers a and b such that $am + bn = 1$.

For the base case, if $n \leq m$ and $n = 0$, then to have n and m coprime we need $m = 1$. In this case we can take $a = 1$, $b = 0$. For the inductive step, assume m and n are coprime natural numbers, and the result is true for all coprime natural numbers m', n' with $m' + n' < m + n$. Swapping m and n if necessary, we can assume $n \leq m$. We have already proven the result for $n = 0$, so assume $n > 0$. By Theorem 10.1, $n' := n$ and $m' := m - n$ are coprime, and since $n > 0$, $m' + n' = m < m + n$. By the induction hypothesis (note that

[20]As exemplified by $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$.

$m' \in \mathbb{N}$), there exists integers a' and b' such that $a'm' + b'n' = 1$, i.e. $a'(m-n) + b'n = 1$, so $a'm + (b'-a')n = 1$. Take $a := a'$, $b := b' - a'$ to get the result. □

Example 10.4. 15 and 8 are coprime, and $(-1) \cdot 15 + 2 \cdot 8 = 1$.

Intuitively, Bézout's lemma says that two coprime integers n and m are very independent in the sense that any integer can be written as an integer combination of n and m.

We now turn to the question of when a number that divides a product divides one of the factors. Recall that this is not true in general (4 divides $2 \cdot 2$ but 4 does not divide 2).

Theorem 10.5. Assume m, n, k are integers. If m and n are coprime and m divides nk, then m divides k.

Proof. By Bézout's lemma, there are integers a and b such that $am + bn = 1$. Multiplying both sides of this equation by k, we get that $amk + bnk = k$. Now m divides amk, and m divides ank (since it divides nk by assumption), so by Theorem 10.1, it must divide the sum, i.e. m divides k. □

A simple consequence is:

Theorem 10.6 (Euclid's lemma)**.** Assume n and k are integers and p is prime. If p divides nk, then either p divides n or p divides k. More generally, if p divides $n_0 n_1 \dots n_r$, then p divides n_i for some i.

Proof. Assume p does not divide n. Then p and n must be coprime, so we can apply the previous theorem (with $m = p$). The general case now follows by an easy induction (exercise). □

We can now prove:

Theorem 10.7 (The fundamental theorem of arithmetic)**.** Any natural number $n \geq 2$ can be uniquely written as a product of primes (up to re-ordering of the factors).

Proof. We have already proven existence (Theorem 7.18). We prove uniqueness by strong induction on n. The base case is when $n = 2$ (or more generally when n is prime) and is true by definition of a prime number. For the inductive step, assume $n = p_0 p_1 \dots p_m = q_0 q_1 \dots q_r$, where the p_is and q_is are prime and $m, r \geq 1$. Now by Theorem 10.6, p_0 divides q_i for some i. Since q_i is prime, this means that $p_0 = q_i$. By re-ordering the q_js, we can assume $i = 0$, i.e. $q_0 = p_0$. Applying the induction hypothesis on $p_1 p_2 \dots p_m = \frac{n}{p_0} = \frac{n}{q_0} = q_1 q_2 \dots q_r$, we get that the lists $p_1, p_2, \dots, p_m$ and $q_1, q_2, \dots, q_r$ must be the same up to

re-ordering (so in particular $m-1=r-1$, so $m=r$). Thus the list $p_0, p_1, \ldots, p_m$ and $p_0 = q_0, q_1, \ldots, q_r$ are also the same. This concludes the proof of uniqueness. □

Remark 10.8. We can also see 1 as the unique product of no primes at all (the empty product). With this convention, we obtain that every positive natural number is a unique product of primes.

10.2. **The Euclidean algorithm.** How can we compute the coefficients a and b in Bézout's lemma? To see this, introduce the concept of a *greatest common divisor*

Definition 10.9. For integers m and n, the *greatest common divisor (gcd)* of m and n, written $\gcd(m,n)$ is the maximal number that divides both m and n. If $m=n=0$, there is no such maximum, so we define $\gcd(0,0) := 0$.

Example 10.10. $\gcd(15,20) = 5$, $\gcd(8,15) = 1$.

Here, lecture 19 ended and lecture 20 started.
Here are some elementary properties of the gcd:

Theorem 10.11. Assume n, m, and k are integers.

(1) $\gcd(n,m) = \gcd(m,n)$.
(2) $\gcd(n,m) = \gcd(\pm n, \pm m)$.
(3) $\gcd(n,m) = \gcd(n, m+kn)$.
(4) $\gcd(n,m) = 1$ if and only if n and m are coprime.
(5) $\gcd(n,m) = 0$ if and only if $n = m = 0$.
(6) If n divides m, $\gcd(n,m) = |n|$. In particular, $\gcd(n,0) = |n|$.
(7) If $n = ka$, $m = kb$, and a and b are coprime, then $\gcd(n,m) = |k|$.

Proof. Exercise (assignment 8). □

From Theorem 10.11.(7), we see that one way to compute the gcd of two positive natural numbers is to multiply the primes that appear in both prime factorizations. However, there is no known general fast method to compute the prime factorization of a number. There *is* a very quick method to compute the gcd though. This relies on Theorem 10.11.(3): instead of computing the gcd of n and m, we can compute the gcd of n and $m-kn$, where of course we should take k so that $m-kn$ is small. There is a natural choice for such k:

Theorem 10.12. For any integers m and n with n nonzero, there exists unique integers k and r such that $m = nk + r$ and $0 \leq r < |n|$. We call k the *quotient* and r the *remainder* of the division of m by n.

Proof. We first prove *existence*. Let's first assume that m and n are non-negative. Take l to be the minimal natural number such that $nl > m$ (such a minimal element exists: since n is nonzero, $n(2m) > m$ and so the set of those l is nonempty. Now use the well-ordering principle). Let $k := l - 1$. Intuitively, we have picked k to be the largest natural number such that $nk \leq m$, which should fit your idea of what the quotient of a division is. Let $r := m - nk$. Let's check they are as desired:

- Since m is non-negative, we must have $l > 0$. Thus $k = l-1$ is a natural number, and by minimality of l we must have $nk \leq m$.
- Therefore $r = m - nk$ is non-negative. Moreover, $nk + r = m < nl = n(k + 1) = nk + n$. Taking away nk from the left hand and right hand sides of this equation, $r < n = |n|$.

We now have proven existence for non-negative m and n. Assume now that at least one of m or n is negative. Let $m' := |m|$, $n' := |n|$. Take k' and r' as given by the previous case such that $m' = k'n' + r'$, $0 \leq r' < |n| = n'$. We consider two cases:

(1) If m is non-negative, then $m = m'$ and n is negative so $n' = -n$ and we can take $r := r'$ and $k' := -k$.
(2) If m is negative, then we have that $m = -m' = -k'n' - r'$. If $r' = 0$, we set $r := r$, $k = -k'$ if n is positive, $k = k'$ otherwise. Otherwise, we cannot allow a negative remainder, so we again consider two cases:
   (a) If n is positive, $n' = n$, so let $k := -k' - 1$, $r := n - r'$. Then $kn + r = (-k' - 1)n + n - r' = -k'n - r' = -k'n' - r' = m$.
   (b) If n is negative, $n' = -n$, so let $k := -(-k' - 1)$, $r := n' - r'$. Then $kn + r = -(-k' - 1)n + (n' - r') = (-k' - 1)n' + (n' - r') = -k'n' - r' = m$.

Next, we show *uniqueness*. Assume we have $m = nk + r = nk' + r'$ for integers r, r', k and k' such that $0 \leq r, r' < |n|$. We show that $k = k'$, from which it must follow that also $r = r'$. Permutting k and k' if necessary, we can assume $k \leq k'$. Find a non-negative l such that $k + l = k'$. Then $m = nk' + r' = n(k + l) + r' = nk + nl + r'$. Thus $r = nl + r'$. If $l = 0$, we are done. So assume for a contradiction that $l > 0$. Then we must also have that $n > 0$ (recall that $n \neq 0$): otherwise since $0 \leq r' < |n| = -n$, $r = r' + ln < -n + ln \leq 0$, which is impossible. But then $n = |n| \leq nl \leq nl + r' = r < |n|$, a contradiction again.

□

Example 10.13.

- $7 = 2 \cdot 3 + 1$ so if $m = 7$ and $n = 3$, we get $k = 2$, $r = 1$.
- $-7 = 3 \cdot (-3) + 2$. So if $m = -7$ and $n = -3$, we get $k = 3$, $r = 2$.

We can now describe the *Euclidean algorithm* for computing the gcd of two integers n and m:

(1) Replace n by $-n$ and m by $-m$ if necessary in order to get $n, m \geq 0$.
(2) Swap n and m if necessary so that $n \leq m$.
(3) If $n = 0$, output m.
(4) Otherwise, $0 < n$, so let k be the quotient and $r := m - nk$ the remainder of the division of m by n. Recursively compute $\gcd(n, r)$ and output it.

Step 1 is correct by Theorem 10.11.(2), step 2 is correct by Theorem 10.11.(1), step 3 is correct by Theorem 10.11.(6), and step 4 is correct by Theorem 10.11.(3). The algorithm terminates because once n and m are natural numbers, the algorithm is only used on natural number values and the sum of those values strictly decreases at each step. In fact, it can be shown that the algorithm terminates after only (approximately) $\log_2(n + m)$ steps.

Example 10.14. Let us compute $g := \gcd(n, m)$ where $n = 1252$ and $m = 3031$. We already have $n \leq m$. We have that $3031 = 2 \cdot 1252 + 527$ so the remainder of the division of 3031 by 1252 is 527, hence $\gcd(1252, 3031) = \gcd(1252, 527)$. We continue in this way: $1252 = 2 \cdot 527 + 198$, so the remainder of the division of 1252 by 527 is 198. Thus $g = \gcd(527, 198)$. Again, $527 = 198 \cdot 2 + 131$ so $g = \gcd(198, 131)$. Next, $198 = 1 \cdot 131 + 67$, so $g = \gcd(131, 67)$. $131 = 1 \cdot 67 + 64$, so $g = \gcd(67, 64)$. $67 = 1 \cdot 64 + 3$, so $g = \gcd(64, 3)$. $64 = 21 \cdot 3 + 1$, so $g = \gcd(3, 1)$. Finally, $3 = 3 \cdot 1 + 0$, so $g = \gcd(1, 0) = 1$.

Note that we never needed to find the prime factorizations of 1252 and 3031. It turns out $1252 = 2 \cdot 2 \cdot 313$ and $3031 = 7 \cdot 433$. What does this have to do with Bézout's lemma? Well, keeping a paper trail of what the Euclidean algorithm exactly does enables us to compute integers a and b such that $1 = a \cdot 1252 + b \cdot 3031$:

Example 10.15. Taking $n = 1252$ and $m = 3031$ again and reversing our steps in the previous example, we know that $64 = 21 \cdot 3 + 1$, so $1 = 64 - 21 \cdot 3$. To make the steps clearer, we will write the numbers that were plugged into the gcd function and must be expanded further in boldface. We have:

$$1 = \mathbf{64} - 21 \cdot \mathbf{3} \tag{1}$$

From the previous step, $\mathbf{67} = 1 \cdot \mathbf{64} + \mathbf{3}$, so $\mathbf{3} = \mathbf{67} - \mathbf{64}$. Plugging this into (1), we get:

$$1 = \mathbf{64} - 21 \cdot (\mathbf{67} - \mathbf{64}) = 22 \cdot \mathbf{64} - 21 \cdot \mathbf{67} \tag{2}$$

We continue backtracking in this way until we obtain the coefficients for 1252 and 3031: we know $\mathbf{64} = \mathbf{131} - \mathbf{67}$, so:

$$1 = 22 \cdot (\mathbf{131} - \mathbf{67}) - 21 \cdot \mathbf{67} = 22 \cdot \mathbf{131} - 43 \cdot \mathbf{67} \tag{3}$$

From the computations in the previous example, we have that $\mathbf{67} = \mathbf{198} - \mathbf{131}$, so:

$$1 = 22 \cdot \mathbf{131} - 43 \cdot (\mathbf{198} - \mathbf{131}) = 65 \cdot \mathbf{131} - 43 \cdot \mathbf{198} \tag{4}$$

Now, $\mathbf{131} = \mathbf{527} - 2 \cdot \mathbf{198}$, so:

$$1 = 65 \cdot (\mathbf{527} - 2 \cdot \mathbf{198}) - 43 \cdot \mathbf{198} = 65 \cdot \mathbf{527} - 173 \cdot \mathbf{198} \tag{5}$$

We have that $\mathbf{198} = \mathbf{1252} - 2 \cdot \mathbf{527}$, so:

$$1 = 65 \cdot \mathbf{527} - 173 \cdot (\mathbf{1252} - 2 \cdot \mathbf{527}) = 411 \cdot \mathbf{527} - 173 \cdot \mathbf{1252} \tag{6}$$

Finally, $\mathbf{527} = \mathbf{3031} - 2 \cdot \mathbf{1252}$, so:

$$1 = 411 \cdot (\mathbf{3031} - 2 \cdot \mathbf{1252}) - 173 \cdot \mathbf{1252} = 411 \cdot \mathbf{3031} - 995 \cdot \mathbf{1252} \tag{7}$$

So if $a = 411$, $b = -995$, we have $1 = am + bn$. This can be checked by a direct calculation.

The algorithm hints that Bézout's lemma generalizes as follows:

Theorem 10.16. For integers m, n, and k, the following are equivalent:

(1) $\gcd(n, m)$ divides k.
(2) There exists integers a and b such that $k = am + bn$.

In particular, there exists integers a and b such that $am + bn = \gcd(n, m)$.

Proof. Exercise (assignment 8). □

Here, lecture 20 ended and lecture 21 started.

10.3. **Modular arithmetic.**

10.3.1. *b-ary representations of natural numbers.* We have seen there are many ways to represent a natural number n. One way is to write it as $1 + 1 + ... + 1$ (with n many ones). We also know from Theorem 10.7 that every natural number greater than 1 can be uniquely written as a product of primes. Yet another representation is to write our number in its decimal (base 10) expansion you are all familiar with. More generally, one can also write the number in another base. Let's revisit what this means:

Definition 10.17. Assume $b \geq 2$ is a natural number, and let n be a natural number. A *base b (or b-ary) representation* of n is a list $a_m, ..., a_0$, for m a natural number, such that:

(1) $n = \sum_{i=0}^{m} a_i b^i$.
(2) $a_i \in \{0, 1, ..., b-1\}$ for all $0 \leq i \leq m$, and $a_m > 0$ if $m > 0$.

Notice that as opposed to the prime factorization, the b-ary representations expresses the number as a *sum* rather than as a *product*.

Example 10.18. The base 10 representation of 543 is given by $5, 4, 3$, since $543 = 3 \cdot 10^0 + 4 \cdot 10^1 + 5 \cdot 10^2$. The base 2 representation of 15 is $1, 1, 1, 1$, since $15 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3$ (check it).

Before proving existence of such a representation, we need

Theorem 10.19. For $b \neq 1$ a real number and m a natural number :

$$\sum_{i=0}^{m} b^i = \frac{1 - b^{m+1}}{1 - b} = \frac{b^{m+1} - 1}{b - 1}$$

Proof. Assignment 4. □

Theorem 10.20. Assume $b \geq 2$ is a natural number and let n be a natural number. Then n has a unique base b representation.

Proof. We first prove the existence of the representation by induction on n, i.e. we use induction on the propositional function $p(x)$ which says "x has a base b representation".
Base case. 0 can be written as $0 \cdot b^0$, so one can take $m = 0$ and $a_0 = 0$ to be the representation.
Inductive step. Assume n has a base b representation $c_m, \ldots, c_0$. We want to find a base b representation of $n + 1$. We consider two cases:

- Case 1: $c_0 = \ldots = c_m = b - 1$. Then we set $a_0 = \ldots = a_m = 0$, and $a_{m+1} = 1$. We show that $a_{m+1}, \ldots, a_0$ is a base b representation of $n + 1$:

$$n = \sum_{i=0}^{m} c_i b^i = \sum_{i=0}^{m} (b-1)b^i = (b-1)\sum_{i=0}^{m} b^i = (b-1)\frac{b^{m+1}-1}{b-1} = b^{m+1} - 1$$

Therefore, $n + 1 = b^{m+1}$, proving that $a_{m+1}, \ldots, a_0$ is indeed a representation of $n + 1$.

- Case 2: $c_t < b - 1$ for some t. Pick the smallest such t. Then the base b representation of n is of the form $c_m, \ldots, c_{t+1}, c_t, b - 1, \ldots, b - 1$. Set $a_0 = \ldots = a_{t-1} = 0$, $a_t = c_t + 1$, and $a_i = c_i$ for $i > t$. We claim this forms a base b representation for $n + 1$ (that is, the base b representation of $n + 1$ is of the form $c_m, \ldots, c_{t+1}, c_t + 1, 0, \ldots, 0$). This can similarly be checked as above:

$$\begin{aligned} n &= \sum_{i=0}^{m} c_i b^i \\ &= \sum_{i=0}^{t-1} c_i b^i + \sum_{i=t}^{m} c_i b^i \\ &= (b-1)\sum_{i=0}^{t-1} b^i + \sum_{i=t}^{m} c_i b^i \\ &= b^t - 1 + \sum_{i=t}^{m} c_i b^i \\ &= (c_t + 1)b^t - 1 + \sum_{i=t+1}^{m} c_i b^i \end{aligned}$$

So

$$n + 1 = (c_t + 1)b^t + \sum_{i=t+1}^{m} c_i b^i = \sum_{i=t}^{m} a_i b^i = \sum_{i=0}^{m} a_i b^i$$

as needed.

This proves existence of the representation. For uniqueness, assume not and let n be a minimal natural number that has (at least) two different b-ary representations, say $a_m, \ldots, a_0$ and $c_r, \ldots, c_0$. By symmetry, we can assume $m \leq r$. If $m < r$, then we have

$$n = \sum_{i=0}^{m} a_i b^i \leq \sum_{i=0}^{m} (b-1)b^i = b^{m+1} - 1 < b^r$$

and since by definition of a representation $c_r > 0$, $n \geq b^r$, a contradiction. Therefore, $m = r$. Now if $m = 0$, the representations must be the same, so we also have $m > 0$, and so $a_m, c_m > 0$. Now $a_m - 1, ..., a_0$, $c_m - 1, ..., c_0$ are distinct representations (removing the first digit if it is zero) for the number $n - b^m$, contradicting minimality of n. □

You should convince yourself that the least significant digit in the b-ary representation of a number n is the remainder of the division of n by b. It turns out that those remainders interact quite well with integer addition and multiplication. To study this more carefully, we revisit the relation introduced in Example 8.11.(2):

Definition 10.21. Fix an integer n. For integers x and y, we say $x \equiv y \bmod n$ (said "x is congruent to y modulo n") if n divides $x - y$. As usual, we write $x \not\equiv y \bmod n$ if it is not true that $x \equiv y \bmod n$.

For a fixed natural number, we have already observed that this is an equivalence relation. We also discussed that for $n = 0$ and $n = 1$, this relation is not very interesting (if $n = 0$, this is just regular equality and if $n = 1$, any two integers are congruent). Moreover, $x \equiv y \bmod n$ if and only if $x \equiv y \bmod -n$ (signs do not influence divisibility), so we will really only be interested in this relation for $n \geq 2$. Observe that $x \equiv 0 \bmod n$ precisely when n divides x.

Example 10.22.

(1) $42 \equiv 2 \bmod 5$.
(2) $-42 \equiv -2 \equiv -2 + 5 \equiv 3 \bmod 5$.

The reason this relation is so important is that it plays very well with addition and multiplication:

Theorem 10.23. Fix an integer n. Assume x_1, x_2, y_1, y_2 are integers such that $x_1 \equiv x_2 \bmod n$ and $y_1 \equiv y_2 \bmod n$. Then:

(1) $x_1 + y_1 \equiv x_2 + y_2 \bmod n$.
(2) $x_1 y_1 \equiv x_2 y_2 \bmod n$.

Proof. By assumption, we have that n divides $x_2 - x_1$ and n divides $y_2 - y_1$.

(1) We have to see that n divides $x_2 + y_2 - (x_1 + y_1) = (x_2 - x_1) + (y_2 - y_1)$. Since n divides both terms, it must divide the sum.
(2) Pick integers k and m such that $nk = x_2 - x_1$ and $mn = y_2 - y_1$. Then $x_1 = x_2 - nk$, $y_1 = y_2 - mn$, so:

$$x_1 y_1 = x_2 y_2 - x_2 mn - y_2 nk + n^2 mk = x_2 y_2 + n(-x_2 m - y_2 k + nmk)$$

Therefore $x_1y_1 - x_2y_2 = nc$ for $c := -x_2m - y_2k + nmk$ which is an integer. Hence n divides $x_1y_1 - x_2y_2$, so $x_1y_1 \equiv x_2y_2 \bmod n$. □

Thus we obtain that if m is an integer, $n \neq 0$, then $m \equiv r \bmod n$, where r is the remainder of the division of m by n. To see this, observe that by definition we have that $m = nk + r$ and $nk \equiv 0 \bmod n$. Also, for $b \geq 2$, if $a_m, \ldots, a_0$ is the b-ary representation of a natural number n, then $n \equiv \sum_{i=0}^{m} a_i b^i \bmod b$, and since $b \equiv 0 \bmod b$, $n \equiv a_0 \bmod b$. That is, n is congruent modulo b to the least significant digit of its b-ary representation. As another example, we demonstrate a trick to determine divisibility by 9:

Theorem 10.24. A natural number n is divisible by 9 if and only if the sum of its decimal digits is divisible by 9.

Proof. Let $a_m, \ldots, a_0$ be the decimal representation of n. We have that $10 \equiv 1 \bmod 9$, and therefore $10^i \equiv 1 \bmod 9$ for any natural number i. Therefore:

$$n = \sum_{i=0}^{m} a_i 10^i \equiv \sum_{i=0}^{m} a_i \cdot 1 \bmod 9$$

Therefore $n \equiv 0 \bmod 9$ if and only if $\sum_{i=0}^{m} a_i \equiv 0 \bmod 9$. □

Remark 10.25. Modular arithmetic appears a lot in the real world: computers (or really, any kind of digital counter) sometimes "overflow" when adding one to the largest integer their memory can store. In this case, the result is usually obtained by "going back to 0" (or whatever the lower bound for the representation of integers is). Closer to nature, many cyclic phenomenons can be described using modular arithmetic: time (days of the week, of the year, minutes on a clock), or even space (the earth is round...) are examples.

10.3.2. *A long remark on equivalence classes. This has not been covered in class but is here for your own background*

For $n \geq 1$, there are infinitely many representations for the same number modulo n. For example, $2 \equiv 7 \equiv -3 \equiv 1000000002 \bmod 5$. This is sometimes inconvenient and we would like to work with unique representations. You might suggest to always work with the remainder of the division by n, but for example the remainder of the division of 7 by 5 is 2, and the remainder of the division of 8 by 5 is 3, yet the remainder of the division of $7 \cdot 8 \equiv 2 \cdot 3 \equiv 1 \bmod 5$ is 1 which is not $2 \cdot 3 = 6$. Instead, we will work with our friends from assignement 5: equivalence classes.

Fix an integer n. Recall that the equivalence class of the integer x under the relation of congruence modulo n is the set of all integers y such that $x \equiv y \bmod n$. The notation that we previously introduced was $[x]_E$, where E is congruence modulo n, but this is a bit bulky, so we will write $\bar{x}$ for the equivalence class of x modulo n. Note that this implicitly depends on n, even though it is not present in the notation. Thus n should be made clear from context.

We write $\mathbb{Z}_n$ for the set of equivalence classes modulo n (this is often called $\mathbb{Z}/n\mathbb{Z}$, and in assignment 5 this was called A/E for $A = \mathbb{Z}$ and E congruence modulo n).

For example, if $n = 3$, $\bar{0}$ is the set of all elements congruent to 0 modulo 3, i.e. $\bar{0} = \{0, 3, -3, 6, -6, 9, \ldots\} = \bar{3}$. Similarly, $\bar{1} = \{1, -2, 4, -5, 7, 10, \ldots\} = \bar{4}$ and $\bar{2} = \{2, -1, 5, -4, 8, -7, 11, \ldots\}$. Thus we have that $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. In general, for $n > 0$, $|\mathbb{Z}_n| = n$ as the only possible remainders of the division of a number by n are $\{0, 1, \ldots, n-1\}$.

We can define multiplication and addition between equivalence classes in the natural way:

Definition 10.26. Fix an integer n. For integers x and y, we define an addition and a multiplication on $\bar{x}$ and $\bar{y}$ as follows:

(1) $\bar{x} + \bar{y} = \overline{x + y}$.
(2) $\bar{x} \cdot \bar{y} = \overline{x \cdot y}$.

This makes sense by Theorem 10.23: if we have $\overline{x_1} = \overline{x_2}$ and $\overline{y_1} = \overline{y_2}$, then $\overline{x_1 + x_2} = \overline{y_1 + y_2}$. In other words, the definition of addition does not depend on which integer x in the equivalence class we picked. The same remark applies to multiplication.

In this way we obtain a structure with n elements ($\mathbb{Z}_n$), in which we can do addition and multiplication in a way that respects many of the axioms of real numbers. Of course, the elements of $\mathbb{Z}_n$ are *not* real numbers, so there are some differences as well (for example, there is no good way of defining an ordering on $\mathbb{Z}_n$). Yet we will see that for prime ns, $\mathbb{Z}_n$ behaves like the reals as far as addition and multiplication is concerned.

Here, lecture 21 stopped and lecture 22 started.

10.3.3. *Division in modular arithmetic.* We know we can add and multiply fine even in modular arithmetic. We can also subtract, since the negative of an integer is also an integer. What about division? At first glance, this seems to be a nonsensical question: $\frac{1}{4}$ is not even an integer so how would we make sense of dividing 1 by 4 (say modulo 5)? Well, recall how division was defined for the real numbers: we first defined

the *reciprocal* of a number x to be a number y such that $xy = 1$. This definition also makes sense in our context:

Definition 10.27. Fix an integer n and an integer x. We say an integer y is an *inverse* of x modulo n if $xy \equiv 1 \bmod n$. In this case, we write $x^{-1} \equiv y \bmod n$. If x has an inverse, we can then "divide" an integer z by x modulo n by looking at zx^{-1} modulo n.

Remark 10.28. In this notation, x^{-1} is *not* the same as the real number $\frac{1}{x}$ (which we called the reciprocal of x): as noted before, something like $\frac{1}{4} \equiv -1 \bmod 5$ does not make any sense: congruence modulo 5 is defined for integers only. In this course, we will always use the word *reciprocal* for x^{-1} in the real numbers, and *inverse* for x^{-1} modulo n.

Example 10.29.

(1) An inverse of 4 modulo 5 is 4: $4 \cdot 4 \equiv 16 \equiv 1 \bmod 5$. An inverse of 3 modulo 7 is 5: $3 \cdot 5 \equiv 15 \equiv 1 \bmod 7$. We also have that -2 is an inverse of 3 modulo 7 (because $-2 \equiv 5 \bmod 7$).
(2) As with the real numbers, for $|n| \neq 1$, 0 never has an inverse modulo n.
(3) Even though it is nonzero, 2 does not have an inverse modulo 4: this can be seen by trying all possible candidates (there are only four of them: $0, 1, 2, 3$). For any integer y either $2y \equiv 0 \bmod 4$ or $2y \equiv 2 \bmod 4$. This can be explained by the fact that 2 is even, so there is no way to multiply it by something that would produce an odd remainder to the division by 4.

Thus we see that inverses need not exist, even for nonzero numbers. Before studying the question of existence further though, let's think about uniqueness. In the sense of pure equality, inverses are not unique (as demonstrated by the first example). However, they are unique modulo n:

Theorem 10.30 (Uniqueness of inverses modulo n)**.** For a fixed integer n, if y and y' are inverses of x modulo n, then $y \equiv y' \bmod n$.

Proof. By definition, we have that $xy \equiv 1 \bmod n$. Multiplying both sides of this equation by y', we get that $y'xy \equiv y' \bmod n$. Now $y'x \equiv 1 \bmod n$ by definition of y', so $y \equiv y' \bmod n$. □

Let's now think about existence of inverses. We saw that 2 does not have an inverse modulo 4. It turns out this is related to the fact that 2 shares a common factor with 4, and that this is the only obstacle:

Theorem 10.31 (Existence of inverses modulo n)**.** Fix an integer n. If x and n are coprime, then x has an inverse modulo n.

Proof. By Bézout's lemma, there exists integers a and b such that $ax + bn = 1$. Thus $ax - 1 = -bn$, i.e. $ax \equiv 1 \bmod n$. Therefore a is an inverse of x. □

Note that the proof also tells us how to *compute* an inverse: just use the Euclidean algorithm to obtain integers a and b so that $ax + bn = 1$. Then a is an inverse of x modulo n.

Thus we conclude that things work especially well when n is prime:

Theorem 10.32. Assume p is a prime and x is an integer. If $x \not\equiv 0 \bmod p$, then x has an inverse modulo p.

Proof. If $x \not\equiv 0 \bmod p$, then p does not divide x, so x and p are coprime and the result follows from the previous theorem. □

Example 10.33. We can solve the modular equation: $51x \equiv 42 \bmod 11$ (for $x \in \mathbb{Z}$) as follows: first we can reduce 42 to -2 modulo 11, and 51 to -4 modulo 11, so the equation becomes $(-4)x \equiv 2 \bmod 11$, or (multiplying both sides by -1), $4x \equiv 2 \bmod 11$. First note that the solution is *not* $\frac{1}{2}$ (this is not an integer). To get an integer solution, we find an inverse of 4 modulo 11 (such an inverse must exist since 11 is prime). We could use the Euclidean algorithm to compute the gcd of 4 and 11, but we instead use trial and error to establish that $4 \cdot 3 \equiv 1 \bmod 11$, hence 3 is an inverse of 4 modulo 11. Multiplying both sides of the equation by 3, we obtain $x \equiv 6 \bmod 11$. This is the only solution (modulo 11) by uniqueness of inverses modulo 11. The set of integer solutions can be described by $\{x \in \mathbb{Z} \mid x = 6 + 11k \text{ for some } k \in \mathbb{Z}\}$.

10.4. **Two important theorems.** What if we want to solve *systems* of linear equations like $ax \equiv m_1 \bmod n_1$, $bx \equiv m_2 \bmod n_2$? The general case is a bit annoying to state (e.g. because we first need to know each equation individually has a solution), but the most fundamental result is:

Theorem 10.34 (The Chinese remainder theorem)**.** Assume $n_0, m_0, n_1, m_1, \ldots, n_k, m_k$ are integers. Assume that $n_0, n_1, \ldots, n_k$ are pairwise coprime. Then there exists an integer x satisfying the system of equations:

$$\begin{aligned} x &\equiv m_0 \bmod n_0 \\ x &\equiv m_1 \bmod n_1 \\ &\cdots \\ x &\equiv m_k \bmod n_k \end{aligned}$$

Furthermore, x is unique modulo $n_0 n_1 \ldots n_k$.

Proof. The result is clear for $k = 0$ so assume $k \geq 1$. Let's first prove existence. We will take x to be of the form $\sum_{i=0}^{k} m_i b_i$, where b_i is such that $b_i \equiv 1 \bmod n_i$ but $b_i \equiv 0 \bmod n_j$ for $j \neq i$. You should convince yourself that such an x will work. Let's see how to find the b_is.

For i between 0 and k, define $a_i := \prod_{j \neq i} n_j$ (i.e. we take the product of all the n_js except n_i). We have that a_i and n_i are coprime (if a prime p divides a_i and n_i, then by Theorem 10.6 it must divide some n_j with $j \neq i$, and so n_i and n_j are not coprime, which contradicts the pairwise coprime assumption). Thus a_i has an inverse modulo n_i. Let c_i be such an inverse, and let $b_i := a_i c_i$. Then the b_is are as desired: $b_i \equiv 1 \bmod n_i$ by definition of an inverse, but $a_i \equiv 0 \bmod n_j$ for $j \neq i$, so also $b_i \equiv 0 \bmod n_j$.

To see uniqueness, assume x and x' are solutions to the system. We have that for each i, $x \equiv x' \bmod n_i$, so n_i divides $x - x'$. Since the n_is are pairwise coprime, they share no common prime factors, and so we must also have that $n_0 n_1 \dots n_k$ divides $x - x'$, i.e. $x \equiv x' \bmod n_0 n_1 \dots n_k$. □

The name "Chinese remainder" comes from the fact that generals in ancient China would use this theorem to count their soldiers: soldiers would be asked to line up in rows of n_0 soldiers, and then in rows of n_1 soldiers for n_0, n_1 coprime integers. The general would only count the number of soldiers in the last row and deduce the total number of soldiers. You will have the opportunity to explore this application further in assignment 9.

Here, lecture 22 ended and lecture 23 started.

Another very useful theorem is about exponentiation:

Theorem 10.35 (Fermat's little theorem)**.** Assume p is prime and x is an integer. Then $x^p \equiv x \bmod p$. If $x \not\equiv 0 \bmod p$, then $x^{p-1} \equiv 1 \bmod p$.

Proof. The first part is a reformulation of problem 3 in assignment 8. For the second part, simply multiply the equation $x^p \equiv x \bmod p$ by an inverse of x modulo p (exists as x is not zero modulo p). □

Remark 10.36. The adjective "little" is used to distinguish Fermat's little theorem from *Fermat's last theorem*, a much harder result which was only proven more than 300 years after Fermat by Andrew Wiles. It says that there is no positive integer solution to the equation $x^n + y^n = z^n$ when $n \geq 3$ is a natural number.

Example 10.37. Fermat's little theorem lets us do modular exponentiation very quickly. For example, let's compute the remainder of the division of 47^{88} by 7. This is congruent to $5^{88} \bmod 7$. Now,

$88 = 4 + 14 \cdot 6$, so $5^{88} = 5^{4+14\cdot 6} = 5^4 \cdot (5^6)^{14}$. By Fermat's little theorem, $5^6 \equiv 1 \bmod 7$, so we only have to compute $5^4 \bmod 7$. A useful method for this is *repeated squaring*: $5^2 \equiv 25 \equiv 4 \bmod 7$, and so $5^4 = (5^2)^2 \equiv 4^2 \equiv 16 \equiv 2 \bmod 7$.

Example 10.38. Fermat's little theorem also lets us prove quickly that a number n is *not* prime. Let's for example take $n = 341$. To see whether it is prime, one *could* check all possible divisors. This is okay for such a small number but would take a ridiculous amount of time for larger numbers. On the other hand, the *contrapositive* of Fermat's little theorem tells us that if we can find an integer x such that $x^{341} \not\equiv x \bmod 341$, then 341 is not prime. Let's compute the remainder of 7^{341}. We could use repeated squaring, but we can get away with less: $7^3 \equiv 343 \equiv 2 \bmod 341$, so $7^{341} \equiv 7^{3\cdot 113+2} \equiv 2^{113} \cdot 7^2 \bmod 341$. Now $2^{10} \equiv 1024 \equiv 1 \bmod 341$, so $2^{113} \equiv 2^{110}2^3 \equiv 8 \bmod 341$, and $7^2 \equiv 49 \bmod 341$. Thus $7^{341} \equiv 8 \cdot 49 \equiv 392 \equiv 51 \bmod 341$. Since $51 \not\equiv 7 \bmod 341$ this shows us that 341 is not prime. Indeed, it turns out $341 = 11 \cdot 31$.

Remark 10.39. The method above does not always work: there are numbers n such that $x^n \equiv x \bmod n$ for all x, but n is not prime. These are called *Carmichael numbers*. An example is 561 (which is divisible by 3).

10.5. **Application: the RSA cryptosystem.** Most of the material in this subsection was taken from [Wikc].

In his famous book [Har92], the mathematician G.H. Hardy declared that number theory was the purest part of pure mathematics, and was unlikely to ever have any practical application. The development of sophisticated communication systems later proved him wrong.

Consider the following problem: Alice and Bob want to privately communicate through some communication channel (for example a phone or the internet), but they know that the channel is monitored and that everything they say will be listened to. We assume Alice and Bob cannot meet physically (maybe Alice lives in New York and Bob lives in Paris): all their communications must happen through the monitored channel. We assume the eavesdropper can *listen* to what Alice and Bob say, but cannot modify the content of their conversation. On networks such as the internet, such a situation is very common (ebanking, shopping, private email/chat, evoting, connecting to your andrew account...), although the assumption that the eavesdropper cannot change the data in transit does not always hold.

You should convince yourself that Alice and Bob cannot simply agree on some secret code over their communication channel: the secret code

would be picked up by the eavesdropper. Amazingly, there is still a way Alice and Bob can communicate securely (or at least, nobody has figured out how to break that scheme yet). This is the *RSA cryptosystem*, named after its inventors: Rivest, Shamir, and Adleman. This is one of the most widely used cryptosystem on the internet: every time you see "https" in the address bar of your browser, RSA is likely being used in some way.

Warning: the scheme described below is oversimplified and has several flaws that an actual implementation must address. Do not try to use it as given to communicate securely.

Let's describe how Alice can send a private message to Bob (the symmetric method will allow Bob to reply to Alice). Before going into the number-theoretic details, we give a physical analogy: assume Alice and Bob could use the (physical) mail system. In this case, Bob buys a very strong lock and sends an empty suitcase, together with the (open) lock, to Alice. Crucially, Bob keeps the lock's key. In this way anybody who intercepts the suitcase only gets a worthless lock and no key to open it once closed. Alice puts her secret message in the suitcase, and closes it using the lock. Note that she does not need the lock's key to do this. She then sends the suitcase back to Bob. On transit, nobody can open the lock (it is very strong). Bob receives the suitcase and can open it since he kept the lock's key.

In our case, the lock and the key will be coded by numbers. We will call the lock Bob's *public key* (anybody, including Alice or the eavesdropper, can see it and use it to send Bob locked suitcases), and its key will be called Bob's *private key* (only Bob has it and he never sends it out, even to Alice).

Key generation. To allow her to communicate, Bob must first send some data (the lock and suitcase in the physical analogy) to Alice: he randomly chooses two large distinct primes p and q (although we will not go into the details, there are algorithms to do this). By "large", we mean about a thousand decimal digits. Bob computes $n := pq$, $n' := (p-1)(q-1)$, and picks a natural number $2 \leq e < n'$ coprime to n' (a prime not dividing n' would work for example). Bob sends n and e to Alice (but, crucially, keeps p, q, and n' secret). We refer to the pair (n, e) as Bob's *public key*. The triple (p, q, n') is refered to as Bob's *private key*. Of course, the eavesdropper will also know the public key (n, e). However, no efficient way is currently known to deduce n', p or q from (n, e) (in particular, no efficient way is known to factor n into p and q), so we assume Bob is the only one to know (n', p, q).

Encryption. Now, we assume the message Alice wants to send to Bob can be coded as a finite string of 0s and 1s, and therefore as a number

m. We assume further that the message is coded in such a way that $2 \leq m < n$ (if not, Alice can always split her message into smaller parts and repeat the scheme).

Of course, m is secret and so Alice can't just send m over the communication channel. Instead, she sends some *cyphertext* $c \equiv m^e \bmod n$ (for example, c could be the remainder of the division of m^e by n). It is possible for Alice to compute such a c since Bob previously sent her n and e. The computation can be done quite efficiently using repeated squaring. However, with only n and e, no efficient way is known to revert the process, i.e. get back m from $m^e \bmod n$ (This is known as the *discrete logarithm problem*. Of course, e should be taken sufficiently large so that $m^e > n$). Thus the eavesdropper cannot do anything with c, n and e alone.

Decryption. Recall however that Bob also kept secret his private key (n', p, q). To recover m from c, Bob computes an inverse d of e modulo n' (it exists since e was chosen coprime to n' and can be computed efficiently using the Euclidean algorithm), and computes c^d modulo n. Note that since nobody but Bob knows n', Bob is also the only one to know d.

We claim that this works: $m \equiv c^d \equiv m^{ed} \bmod n$.

To prove this, we use the Chinese remainder theorem: recall $n = pq$, with p and q distinct primes. In particular, they are coprime and so it is enough to see $m \equiv m^{ed} \bmod p$ and $m \equiv m^{ed} \bmod q$ separately (because then m^{ed} and m are both solutions to the system of equations $x \equiv m^{ed} \bmod p$ and $x \equiv m^{ed} \bmod q$, so by the uniqueness part of the Chinese remainder theorem, $m \equiv m^{ed} \bmod pq = n$). Let's see $m \equiv m^{ed} \bmod p$, and the proof for q will be symmetric.

First observe that if $m \equiv 0 \bmod p$, then $m^{ed} \equiv 0 \equiv m \bmod p$, as desired. So we can assume $m \not\equiv 0 \bmod p$.

Recall that d is an inverse of e modulo $n' = (p-1)(q-1)$, so $ed \equiv 1 \bmod n'$, i.e. for some integer h, $hn' = ed - 1$, or $ed = hn' + 1$. Thus:

$$m^{ed} \equiv m^{hn'+1} \equiv m^{h(p-1)(q-1)+1} \equiv (m^{p-1})^{h(q-1)} \cdot m \bmod p$$

By Fermat's little theorem, $m^{p-1} \equiv 1 \bmod p$ (this is where we are using $m \not\equiv 0 \bmod p$), hence $m^{ed} \equiv m \bmod p$, as desired.

Here, lecture 23 ended and lecture 24 started.

11. Probability

Probability is an important mathematical tool which is used to analyze *uncertainty*. Some of its results sometimes run counter to our intuition. We will for example explore the three following problems:

(1) A family with two children has at least one boy. What is the probability that the other child is also a boy?
(2) Thirty students sit in a room. What is the probability that two of them share the same birthday?
(3) In every single course, the math majors have performed better than the English litterature majors. Did the math majors also perform better overall?

Try to answer each before reading on! Hint: They are tricky. The answer to some even depends on how we interpret them.

11.1. **Defining probabilities.** Precisely defining "probability" is complicated. The simplest example of a probabilistic event is that of tossing a coin: Experience shows that if we toss a coin n times, it will fall on head roughly $n/2$ times and fall on tail on the other half of the times. Thus the ratio of the number of heads to the total number of tossing is approximately $1/2$. When n is very large, we expect this ratio to get closer and closer to $1/2$. At the limit, it should be exactly $1/2$. We call this limit the *probability* that a random coin toss falls on head.

Similarly, if we roll a (fair) die we expect to get a six (or any other number) approximately once every six times. Thus we would say that the probability of rolling a six is $1/6$.

We can see the two examples above as performing an experiment (tossing a coin or rolling a die) and associating a probability to each outcome depending on how likely it is to happen. In the examples seen so far, each outcome had the same probability (they were *equally likely*). This need not be the case: we could for example flip a biased coin that is head a quarter of the times and tail the remaining three quarters of the time. We can also ask for the probability of a *set* of outcomes (called an *event*) to happen. For example, experience shows the probability to roll a six *or* a five on a fair die is $2/6 = 1/3$.

Based on those examples, we will use the following *axiomatic* definition of probability:

Definition 11.1. A *finite probability space* is a non-empty[21] finite set S together with a function $P : \mathcal{P}(S) \to \mathbb{R}$ satisfying the following three axioms:

[21]This actually follows from the axioms (can you see why?).

- (P_0) If $A \subseteq S$, $0 \leq P(A) \leq 1$.
- (P_1) $P(S) = 1$.
- (P_2) If A and B are two *disjoint* subsets of S, $P(A \cup B) = P(A) + P(B)$.

P is called the *probability function* of S.
We say S is *uniform* if $P(\{a\}) = \frac{1}{|S|}$ for every $a \in S$.

We see S as the set of outcomes and P as a function that gives the probability that a subset of outcomes (an event) happens. We can also talk about infinite probability spaces, but the situation is much trickier there.

Note that (exactly as in the proof of Theorem 9.1), if A_0, A_1, ..., A_k are pairwise disjoint subsets of S, then $P(A_0 \cup A_1 \cup \ldots \cup A_k) = \sum_{i=0}^{k} P(A_i)$. In particular, if $A = \{a_0, a_1, \ldots, a_k\}$, we have that $P(A) = \sum_{i=0}^{k} P(\{a_i\})$. Thus the probability an event A can be computed from the probabilities of the elements of A. In case the space is uniform, we get that $P(A) = \frac{|A|}{|S|}$, so only the size of A is needed. Question about the space then often translate to counting problems in combinatorics.

Example 11.2.

- We can model the experiment of tossing a fair coin with the finite probability space $S = \{\text{head}, \text{tail}\}$ with probability function $P(\{\text{head}\}) = P(\{\text{tail}\}) = \frac{1}{2}$ (and with other values defined in the only possible way as described above). This is a uniform probability space. If we instead specify $P(\{\text{head}\}) = \frac{1}{4}$ and $P(\{\text{tail}\}) = \frac{3}{4}$ we obtain a non-uniform probability space.
- We can also model the experiment of rolling a fair die with $S = [6]$, $P(\{i\}) = \frac{1}{6}$ for $i \in [6]$. This is a uniform probability space.
- Consider the more complicated experiment of rolling *two* fair dice. We can model it with the probability space $S = [6] \times [6]$ and the uniform probability function ($P(\{(i,j)\}) = \frac{1}{36}$ for $i, j \in [6]$. For $n \in [12]$, let A_n denote the event that the sum of the two die is n. There is only one way to get a 12: $(6,6)$, so $P(A_{12}) = \frac{1}{36}$, but there are for example two ways to get an 11: $(5,6)$ and $(6,5)$. Thus $P(A_{11}) = \frac{2}{36} = \frac{1}{18}$. You should convince yourself that the most likely sum is 7, as it can happen in 6 possible ways: $(1,6)$, $(2,5)$, $(3,4)$, $(4,3)$, $(5,2)$, $(6,1)$. Thus $P(A_7) = \frac{6}{36} = \frac{1}{6}$. As an exercise, you should figure out the probability of the other A_is.

We will very quickly drop the formalism: We will often write events in plain English instead of explicitly writing the set, and the probability space will often be left implicit.

Before proving some elementary properties of probability spaces, we need to define the complement of a set. Note that this depends on the probability space we are working in.

Definition 11.3. Assume S is a finite probability space. For $A \subseteq S$, the *complement* A^c of A is the set $S \backslash A$ of elements of S not in A.

Theorem 11.4 (Elementary properties of probability spaces)**.** Assume S is a finite probability space with probability function P. Assume $A, B \subseteq S$.

(1) $P(A^c) = 1 - P(A)$.
(2) $P(\emptyset) = 0$.
(3) $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

Proof.

(1) It is easy to check that $S = A \cup A^c$, and A and A^c are disjoint, therefore by axiom (P_2) of probability spaces, $P(S) = P(A \cup A^c) = P(A) + P(A^c)$. By axiom (P_1) of probability spaces, $P(S) = 1$. Thus $1 = P(A) + P(A^c)$, i.e. $P(A^c) = 1 - P(A)$.
(2) Take $A = S$ in the previous property and use axiom (P_1).
(3) This is very similar to the proof of the inclusion-exclusion principle you have done in assignment 7. We have that $A = (A \backslash B) \cup (A \cap B)$, and those sets are disjoint. Thus by (P_2), $P(A) = P(A \backslash B) + P(A \cap B)$, so $P(A \backslash B) = P(A) - P(A \cap B)$. Similarly, $P(B \backslash A) = P(B) - P(A \cap B)$. Finally, $A \cup B = (A \backslash B) \cup (A \cap B) \cup (B \backslash A)$, and those three sets are pairwise disjoint, so repeatedly using axiom (P_2):

$$\begin{aligned} P(A \cup B) &= P(A \backslash B) + P(A \cap B) + P(B \backslash B) \\ &= P(A) - P(A \cap B) + P(A \cap B) + P(B) - P(A \cap B) \\ &= P(A) + P(B) - P(A \cap B) \end{aligned}$$

□

Example 11.5. Assume we are rolling two fair dice (i.e. we are in probability space of Example 11.2.(3)). What is the probability that the first die is even or the sum of the two is 7? We could either list all possibilities that this can happen and count them, or compute each event separately: Let A be the event that the first die is even, B the event that the sum is 7.

We have that $P(A) = \frac{1}{2}$ (either by counting all possibilities, or by observing that the probability that the first die is odd must be the same and that those two probabilities must sum to one), and we already observed that $P(B) = \frac{1}{6}$. This does *not* mean that $P(A \cup B) = \frac{1}{2} + \frac{1}{6}$ as the set A and B are not disjoint (e.g. $(4, 3) \in A \cap B$). We have to compute the probability of $A \cap B$. Simply by counting, this is $\frac{1}{12}$ and so we get that $P(A \cup B) = P(A) + P(B) - P(A \cap B) = \frac{1}{2} + \frac{1}{6} - \frac{1}{12} = \frac{1}{2} + \frac{1}{12} = \frac{7}{12}$.

Here, lecture 24 ended and lecture 25 started.

11.2. **The birthday paradox.** Assume n people are in a room (for a fixed $n \in \mathbb{N}$). What is the probability that two of them have the same birthday? We assume that each person has a birthday that falls in one of the 365 days of a year (no February 29th allowed) and that each day is equally likely to be a person's birthday. Formally, we can model this using the probability space $S := {}^{[n]}[365]$ (each outcome is represented by a function $s : [n] \to [365]$ that you can see as a list $s(1)$, $s(2)$, ..., $s(n)$ giving the birthday of each person) with probability function $P(\{s\}) = \frac{1}{|S|}$ (i.e. each possible list is equally likely). We are looking for $P(A)$ where A is the set of lists s where s repeats the same date twice (i.e. s is *not* an injection). We have a lot of experience with counting but it is easier to count injections than non-injection, so we will first compute $P(A^c)$ (the probability that a random s is an injection which is the probability that no two persons share the same birthday).

Since the space is uniform, $P(A^c) = \frac{|A^c|}{|S|}$, so we only have to compute $|A^c|$ and $|S|$, which since we have a lot of experience with counting should be easy:

- $|S| = 365^n$: it is simply the number of ways to choose n out of 365 dates when order matters and repetitions are allowed.
- $|A^c|$ is the number of ways to choose n out of 365 dates when order matters but repetitions are *not* allowed. When $n > 365$, this is 0 (by the pigeonhole principle). When $n \leq 365$, this is $\frac{365!}{(365-n)!} = 365 \cdot 364 \cdot \ldots \cdot (365 - n + 1)$.

In the end we obtain that:

$$P(A^c) = \begin{cases} \frac{365!/(365-n)!}{365^n} = \frac{365 \cdot 364 \cdot \ldots \cdot (365-n+1)}{365^n} & \text{if } n \leq 365 \\ 0 & \text{if } n > 365 \end{cases}$$

So using Theorem 11.4, $P(A) = 1 - P(A^c)$. So we get that if $n > 365$, $P(A) = 1$ which makes sense (the pigeonhole principle tells us that two persons must have the same birthday). But just from the computed

answer, is hard to get a feeling for what happens when $n \leq 365$. Let's assume for example we would like to estimate the number of people we need to get $P(A)$ above $1/2$. To get an estimate for $\frac{365!/(365-n)!}{365^n}$, we first observe that

$$\begin{aligned}\frac{365!/(365-n)!}{365^n} &= \frac{365-0}{365} \cdot \frac{365-1}{365} \cdot \frac{365-2}{365} \cdot \ldots \cdot \frac{365-(n-1)}{365} \\ &= \left(1 - \frac{0}{365}\right) \cdot \left(1 - \frac{1}{365}\right) \cdot \left(1 - \frac{2}{365}\right) \cdot \ldots \cdot \left(1 - \frac{n-1}{365}\right)\end{aligned}$$

To continue, we will use[22]:

Fact 11.6. Assume x is a real number with $0 \leq x \leq 1$. Then $1 - x \leq e^{-x}$, where e is a real number (that we will not define here) such that $2.71 < e < 2.72$.

Using this fact, we get:

$$\begin{aligned}\left(1 - \frac{0}{365}\right) \cdot \left(1 - \frac{1}{365}\right) \cdot \left(1 - \frac{2}{365}\right) \cdot \ldots \cdot \left(1 - \frac{n-1}{365}\right) &\leq e^{-\frac{0}{365}} \cdot e^{-\frac{1}{365}} \cdot \ldots \cdot e^{-\frac{n-1}{365}} \\ &= e^{-\sum_{i=0}^{n-1} \frac{i}{365}} \\ &= e^{-\frac{1}{365}\sum_{i=0}^{n-1} i} \\ &= e^{-\frac{n(n-1)}{2 \cdot 365}}\end{aligned}$$

So we get that $P(A^c) \leq e^{-\frac{n(n-1)}{2 \cdot 365}}$, so $P(A) = 1 - P(A^c) \geq 1 - e^{-\frac{n(n-1)}{2 \cdot 365}}$. So if $1 - e^{-\frac{n(n-1)}{2 \cdot 365}} \geq \frac{1}{2}$, then $P(A) \geq \frac{1}{2}$. Solving for n (we will not discuss the details, but this is straightforward if you know about logarithms and the quadratic formula), we get $n \geq 23$. In general, if we replace 365 by an arbitrary number m, we get that we need to take n around $\sqrt{m}$ in order to make the probability greater than $1/2$.

Even though there is nothing paradoxical about this result, some people find it surprising that the number is so low. As n grows bigger than 23, the probability grows quickly: it is larger than 0.8 for $n = 35$ (the number of students enrolled in this class), and larger than 0.99 when n is 60.

[22]We take as a given that the exponential function exists, see Fact 5.13.

11.3. **Conditional probabilities.** Conditional probabilities describe "restrictions" of experiments. For example, if you roll two dice, you may be interested in the probability that they sum to 7 given that you rolled a 4 with the first die. One has to be very precise when specifying what the restriction is, as illustrated by the following example:

Example 11.7. A family with two children has at least one boy. What is the probability that the other child is also a boy? We assume that each child is either a boy or a girl and that the two outcomes are equally likely.

- One way to interpret this question is that we know one of the following three possibilities is true:
  (1) The two children are boys
  (2) The younger child is a boy and the older one is a girl.
  (3) The younger child is a girl and the older one is a boy.

  In this case, there are only one out of those three possibilities where the other child is a boy, so the required probability is 1/3.
- Another way to interpret this question is that we know one of the two children is a boy (say the oldest one), and we are asking for the probability that the youngest one is also a boy. In that case, the probability is 1/2.

This is yet another example of the ambiguity of plain English. To state the above question more precisely, we now define conditional probability. As always, we are working in a finite probability space S with probability function P.

Definition 11.8. Assume A and B are two events with $P(B) \neq 0$. The probability of A *given* event B (written $P(A|B)$) is defined to be

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Note that if $P(B) = 0$, $P(A|B)$ is left undefined.

Example 11.9. We can model the previous example as an experiment with probability space $S = \{\text{girl}, \text{boy}\} \times \{\text{girl}, \text{boy}\}$, where a pair in S lists the sexes of the children with the youngest child first. The probability function is uniform: for $x \in S$, $P(\{x\}) = \frac{1}{4}$. The event A representing that the family has two boys is the set $\{(\text{boy}, \text{boy})\}$. If we interpret the question as meaning that we know not all children in the family are girls, then we are conditioning with respect to $B = \{(\text{boy}, \text{girl}), (\text{boy}, \text{boy}), (\text{girl}, \text{boy})\}$. If we interpret the question as

meaning that we know that the (say oldest) child is a boy, then we are conditioning with respect to $C = \{(\text{girl}, \text{boy}), (\text{boy}, \text{boy})\}$. It is now easy to check using the definitions that $P(A|B) = \frac{1}{3}$ and $P(A|C) = \frac{1}{2}$.

Example 11.10. If we throw two dice, what is the probability that the second one is a 6 (call this event A) given that the first one is a six (call this event B)? The intuition is that it should be 1/6: the result of the first throw has no influence on the second one. We can compute this formally.

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{1/36}{1/6} = \frac{1}{6}$$

Thus we have that $P(A) = P(A|B)$ and so $P(A \cap B) = P(A|B)P(B) = P(A)P(B)$. We give this condition a name:

Definition 11.11. Two events A and B are called *independent* if $P(A \cap B) = P(A)P(B)$.

Clearly, events are not always independent (as an extreme case, if $B = A$, $P(A \cap A) \neq P(A)^2$ if $0 < P(A) < 1$. Intuitively, being independent means that (if $P(B) \neq 0$) $P(A|B)$ does not depend on B at all:

Theorem 11.12. If A and B are independent and $P(B) \neq 0$, then $P(A|B) = P(A)$.

Proof. By definition, $P(A|B) = \frac{P(A \cap B)}{P(B)}$, and by independence, $P(A \cap B) = P(A)P(B)$, so the result follows. □

Example 11.13 (Simpson's paradox)**.** During a semester, students must take exactly one class which is either "Concepts of mathematics" (21127) or "Medieval litterature" (76330). Assume we are given the following data describing the number of students majoring in math or English who chose and passed each course[23]:

	Passed 21127	Took 21127	Passed 76330	Took 76330
Math majors	150	190	9	10
English majors	20	40	140	160

Let M describe the event that you are a math major, E the event you are an English major. Let A denote the event that you passed the course you selected, T_x that you took course x. We have that for any course x, $P(A|T_x \cap M) > P(A|T_x \cap E)$ (for example, $P(A|T_{21127} \cap M) =$

[23]The numbers were made up and any ressemblance to reality is purely accidental.

$\frac{150}{190} = \frac{15}{19}$, whereas $P(A|T_{21127} \cap E) = \frac{20}{40} = \frac{1}{2}$. Thus for any given class, the math majors did better than the English majors. Does that mean that they did better on average, i.e. does that mean that a greater proportion of math majors passed their class? No: $P(A|M) = \frac{150+9}{200} = \frac{159}{200}$, whereas $P(A|E) = \frac{20+140}{200} = \frac{160}{200}$. The problem is that more English majors took the hard class than math majors did.

The previous example illustrates that we often have data for the conditional probabilities, but not for the unconditioned ones. For example, how would you compute the probability $P(A)$ that you passed? Well, we can derive it from $P(A|M)$ and $P(A|E)$. This technique is called *conditioning*:

Theorem 11.14 (Conditioning)**.** Assume A and B are events with $0 < P(B) < 1$. Then

$$P(A) = P(A|B)P(B) + P(A|B^c)P(B^c)$$

More generally, if $B_0, B_1, \ldots, B_k$ are pairwise disjoint, $0 \neq P(B_i)$ for all i, and $B_0 \cup B_1 \cup \ldots \cup B_k = S$, then:

$$P(A) = \sum_{i=0}^{k} P(A|B_i)P(B_i)$$

Proof. The first part follows from the second by setting $B_0 = B$, $B_1 = B^c$. For the second part, observe that for each i, $P(A|B_i)P(B_i) = P(A \cap B_i)$, and $A = (A \cap B_0) \cup (A \cap B_1) \cup \ldots \cup (A \cap B_k)$ (exercise!). Since the B_is are pairwise disjoint, the sets in the previous union are also pairwise disjoint and thus:

$$P(A) = \sum_{i=0}^{k} P(A \cap B_i) = \sum_{i=0}^{k} P(A|B_i)P(B_i)$$

as needed. □

Going back to the previous example, we have that $M^c = E$, and $P(M^c) = 1 - P(M)$, so $P(A) = P(A|M)P(M) + P(A|E)(1 - P(M))$. Since 200 out of 400 students are math majors, $P(M) = \frac{1}{2}$, so we get that $P(A) = \frac{1}{2}\left(\frac{159}{200} + \frac{160}{200}\right) = \frac{319}{400}$.

We can also try to reverse what we are conditioning on: What is $P(E|A)$, i.e. given that I passed, what is the probability that I am an English major? This is answered by the following:

Theorem 11.15 (Bayes' theorem)**.** Assume A and B are events with $P(A)$ and $P(B)$ nonzero, then:

$$P(B|A) = \frac{P(A|B)P(B)}{P(A)}$$

Proof. We simply use the definition of conditional probability twice:

$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{P(A|B)P(B)}{P(A)}$$

□

Remark 11.16. In practice, conditioning is often used to compute $P(A)$ in the denominator of Bayes' theorem.

Here, lecture 25 ended and lecture 26 started (the birthday paradox is still to be covered)

In the previous example, we have:

$$P(E|A) = \frac{P(A|E)P(E)}{P(A)} = \frac{(160/200) \cdot (1/2)}{319/400} = \frac{160}{319}$$

Bayes' theorem is often very useful to compute results of clinical trials where e.g. you know the number of persons who failed a test for some illness and you want to get the probability that they have the illness (given the effectiveness of the test). You will explore this application in your assignment. We move on to discuss a very puzzling result:

Example 11.17 (The Monty-Hall problem)**.** You are a contestant at a game show and are asked to choose between one of three doors. Behind one of the door is a spaceship, and behind the two other doors are boring math textbooks. You can have whatever is behind the door you choose to open. You randomly pick a door but before you can open it the host opens one of the other doors, revealing a boring math textbook. The host then asks you whether you want to change your choice of door. Should you change?

To model this problem, we assume without loss of generality that you initially picked door number one. The solution is of course symmetric in the other cases. We work on the space $S = [3] \times [3]$, where the first component of the pair gives the door behind which the spaceship is hidden, and the second component is the door that the host opened. We know for example that $P(\{(a, a)\}) = 0$ for all $a \in [3]$, since the host always opens a door that has a boring book behind it, and also $P(\{(a, 1)\}) = 0$ since you picked the first door. On the other hand, it is not that easy to figure out the probability of the other outcomes.

For $i \in [3]$, let H_i denote the event that the host selected door i, and let A_i be the event that the spaceship is behind door i. We want to compute $P(A_1|H_2)$ and $P(A_1|H_3)$ to figure out what the chances are that there is a spaceship behind the first door. Let's compute $P(A_1|H_2)$, and the symmetric computation will give us that $P(A_1|H_3) = P(A_1|H_2)$. By Bayes' theorem, $P(A_1|H_2) = \frac{P(H_2|A_1)P(A_1)}{P(H_2)}$. Now, $P(A_1) = \frac{1}{3}$ since the spaceship is equally likely to be behind each door. Also, $P(H_2|A_1) = \frac{1}{2}$: if there is a spaceship behind the first door, then the host can choose to open either the second or the third door and will do so (we assume) with equal probability.

It remains to compute $P(H_2)$. For this, we condition on the pairwise disjoint events A_1, A_2, and A_3 (note that $S = A_1 \cup A_2 \cup A_3$):

$$P(H_2) = P(H_2|A_1)P(A_1) + P(H_2|A_2)P(A_2) + P(H_2|A_3)P(A_3)$$

We have already figured out what $P(H_2|A_1)P(A_1)$ is. We also know that $P(A_i) = \frac{1}{3}$ for all $i \in [3]$. Now if the prize is behind the second door, then since you picked the first door, the host has no choice but to open door 3. Thus $P(H_2|A_2) = 0$. Similarly, $P(H_2|A_3) = 1$. Thus $P(H_2) = \frac{1}{2} \cdot \frac{1}{3} + 0 + 1 \cdot \frac{1}{3} = \frac{1}{2}$. Putting everything together, $P(A_1|H_2) = \frac{1/6}{1/2} = \frac{1}{3}$. Therefore $P(A_3|H_2) = P(A_1^c|H_2) = 1 - P(A_1|H_2) = \frac{2}{3}$ (it is easy to check that the rule for computing the probability of complements also holds when conditioning).

In conclusion, the spaceship is much more likely to be behind the other door and therefore you should accept the host's offer and change your choice of door. Thus one's initial intuition that there is one chance out of two that door one is right turns out to be completely wrong!

End of lecture 26. An additional application of Bayes' theorem to spam detection was also discussed.

References

[Dij] Edsger Wybe Dijkstra, *Why numbering should start at zero*, Available online. URL: `https://www.cs.utexas.edu/users/EWD/transcriptions/EWD08xx/EWD831.html`.

[Har92] G. H. Hardy, *A mathematician's apology*, Canto, Cambridge University Press, 1992.

[Rus03] Bertrand Russel, *The principles of mathematics*, Cambridge University Press, 1903.

[RW25] Bertrand Russel and Alfred Whitehead, *Principia mathematica*, Cambridge University Press, 1925.

[Wika] Wikipedia, *Definitions of mathematics*, Available online. Last accessed May 3, 2014. URL: https://en.wikipedia.org/w/index.php?title=Definitions_of_mathematics&oldid=598508146.

[Wikb] ———, *Mathematics*, Available online. Last accessed May 3, 2014. URL: https://en.wikipedia.org/w/index.php?title=Mathematics&oldid=603180831.

[Wikc] ———, *RSA (cryptosystem)*, Available online. Last accessed June 15, 2014. URL: https://en.wikipedia.org/w/index.php?title=RSA_%28cryptosystem%29&oldid=612910973.

E-mail address: sebv@cmu.edu

Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA