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. Once the course is over, I aim to keep theses notes (together with the source files) available on my website: `http://math.cmu.edu/~svasey/`.

21-127 Students: please let me know if you find any mathematical mistake or typo (even if it just something very easy to fix, like a missing comma or a misspelling). Extra credit will be given to students who report such mistakes.

Date: May 6, 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, $2 + 3 = 5$").

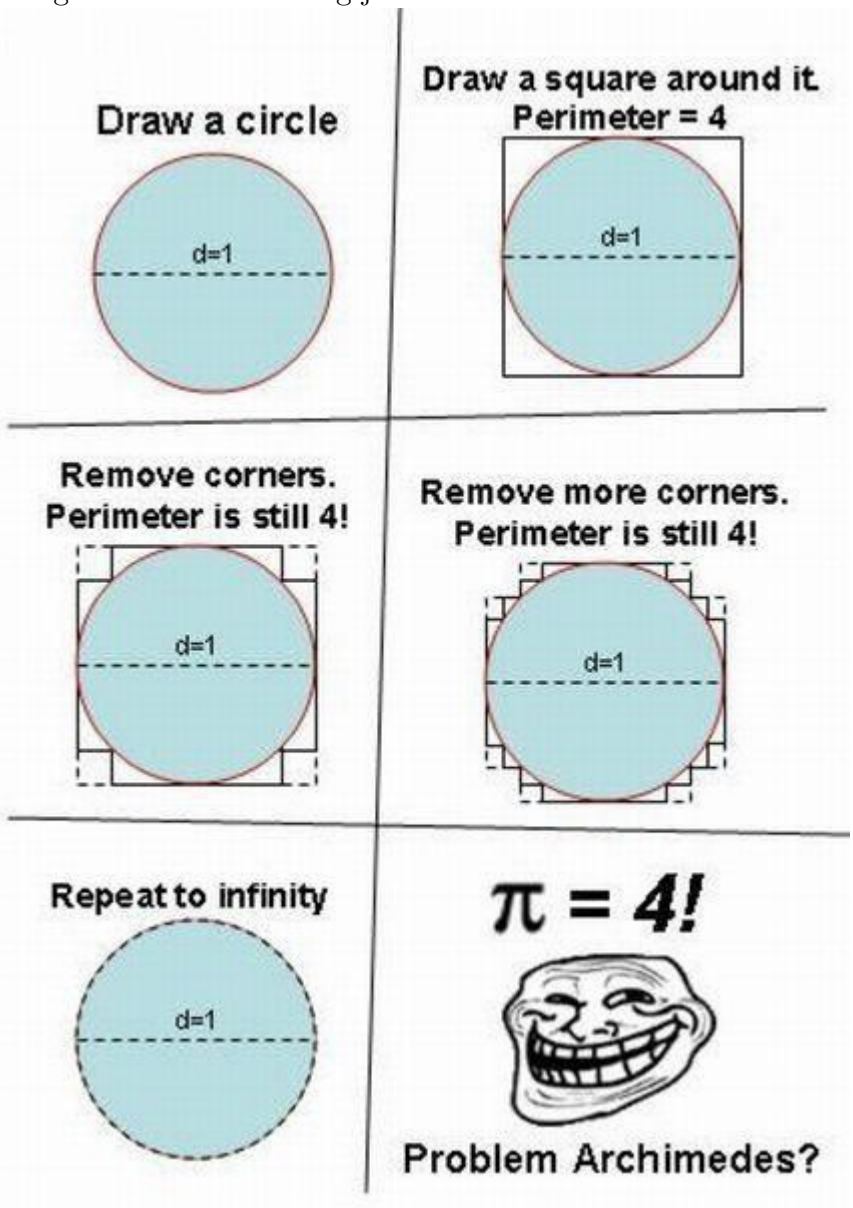
Remark 2.2. On the other hand, there is a danger of writing too much details: this can hurt understanding by burying the most important points of a proof inside pages of easy arguments. An famous extreme case[1] is "Principia Mathematica" [RW25] which takes more than 300 pages to prove that $1 + 1 = 2$ (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 hands, 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 is 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 of course all we have to justify that the "square with removed corners" becomes a circle as we "repeat to infinity" is 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 inverse 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 our 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, $\pi = 3.14159265....$ 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 $1 = 0.999999999....$). 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...) 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.

Fact 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 $x + z < y + z$.
- (C_0) The completeness axiom (*will not be discussed in this course*): If F is a non-empty collection of real numbers and

[6] In this course, a "Fact" is a result which will not be proved but that you can take as a given.

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

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 $0, 1, 2, 3, ...$ (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 $\forall x \exists y\ y^2 = x$. 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:

Fact 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:

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

Where we have used that $y^2 \neq x$ is just a convenient notation for the negation of $y^2 = x$. 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, $y^2 \neq x$, or in other words, there exists a real number that is not the square of any other 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 will cover the entire section (tentative)

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 about.

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 is 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 $r \to q$. . If we know that $\forall x\ p(x)$ is true,

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.

[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.

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.

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).

[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.

(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 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 even. 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) Similar to the previous proofs (exercise).
(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. Thus 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 5.6. 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 5.7. Any integer is either even or odd (but not both by the previous theorem).

From this, we can prove:

Theorem 5.8. 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 5.9. Given a nonzero rational number r, there exists odd integers n and m such that $r = n/m$.

Theorem 5.10. $\sqrt{2}$ 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. Since $\sqrt{2}$ is nonzero, we can use the previous fact to pick *odd* integers n and m such that $\sqrt{2} = \frac{n}{m}$. 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 5.8, n is even. Since we chose n to 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 5.11 (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. □

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 5.12. 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) If y is non-negative, then x^y is positive.
(4) $x^{y+z} = x^y \cdot x^z$.
(5) $(x^y)^z = x^{y \cdot z}$.

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 5.13. 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 5.10).

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

7. Induction

8. Set theory

9. Counting

10. Number theory

11. Probability theory

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.

[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.

E-mail address: sebv@cmu.edu

Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA