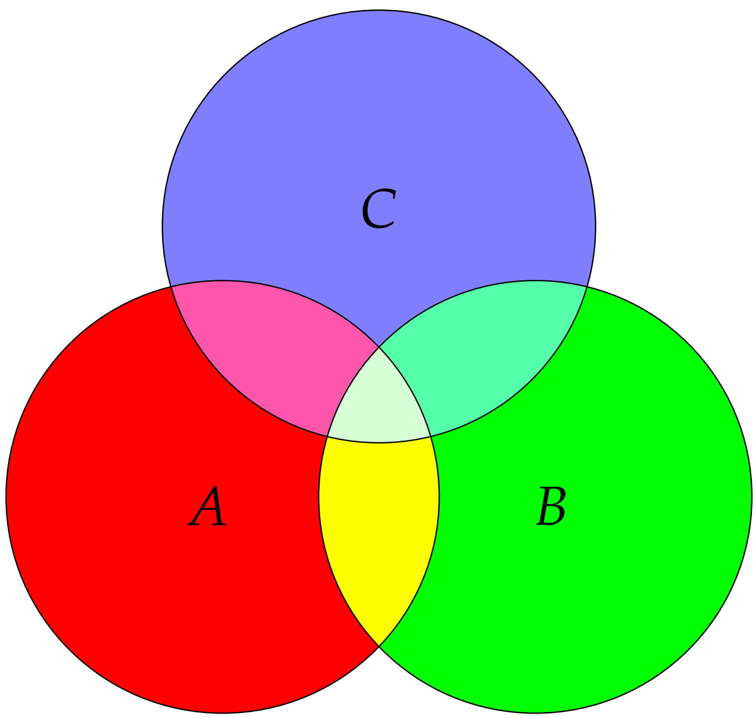
Math 13 — An Introduction to Abstract Mathematics

Neil Donaldson and Alessandra Pantano

With contributions from:
Michael Hehmann, Christopher Davis, Liam Hardiman, and Ari Rosenfield

January 22, 2024



Contents

Preface: What is Math 13 and who is it for?

Math 13 was created by the late Howard Tucker, who chose the number as a joke and to position the class near the end of lower-division. Around 2012, program restructuring positioned Math 13 as the key transition class introducing students to abstraction and proof, and the primary pre-requisite for upper-division pure mathematics.

The typical student is simultaneously working through lower-division calculus and linear algebra. Knowledge of such material is unnecessary and students are encouraged to take the class early so as to ease the transition from algorithmic to abstract mathematics. The skills learned in Math 13 may also be applied beneficially to other lower-division classes.

This text evolved from the first author's course notes dating back to 2008. Math 13 is something of a hydra due to the niche it occupies in UCI's program: part proof-writing, part discrete mathematics, and part introduction to upper-division. Logic is treated more rapidly than in traditional discrete mathematics, with the primary goal of proving mathematical statements as soon as possible; logical algebra is largely delayed until upper-division. Since most students have seen very little abstraction before this class, a deliberate feature is to revisit concepts after the basic ideas have settled; for instance basic set theory is presented long before more advanced ideas such as power sets and infinite cardinalities.

Learning Outcomes

1. Developing the skills necessary to read and practice abstract mathematics.
2. Understanding the concept of proof and becoming acquainted with multiple proof techniques.
3. Learning what sort of questions mathematicians ask and what excites them.
4. Introducing upper-division mathematics by providing a taste of what is covered in several courses. For instance:

   Number Theory Five people take the same number of candies from a jar which contains 239 candies. Seven people then do the same thing. If the jar is now empty, how many candies did each person take?

   Geometry and Topology How can we visualize and compute with objects like the Möbius strip, and how can we use sequences of sets to produce objects that appear similar at all scales?

   To Infinity and Beyond! Why are some infinities greater than others?

Useful Texts The following texts are recommended if you want more exercises and material. The first two are available free online, while the remainder were previous textbooks for Math 13.

- *Book of Proof*, Richard Hammack
- *Mathematical Reasoning*, Ted Sundstrom
- *Mathematical Proofs: A Transition to Advanced Mathematics*, Chartrand/Polimeni/Zhang
- *The Elements of Advanced Mathematics*, Steven G. Krantz
- *Foundations of Higher Mathematics*, Peter Fletcher and C. Wayne Patty

1 Introduction: What is a Proof?

The essential concept in higher-level mathematics is that of *proof.* A basic dictionary entry might cover two meanings:

1. A test or trial of an assertion.
2. An argument that establishes the validity (truth) of an assertion.

In science and the wider culture, the first meaning predominates: a defendant was *proved* guilty in court; a skin cream is clinically *proven* to make you look younger; an experiment *proves* that the gravitational constant is 9.81ms^{-2}. A common mistake is to assume that a *proved assertion* is actually *true.* Two juries might disagree as to whether a defendant is guilty, and for many crimes the truth is uncertain hence the more nuanced legal expression *proved beyond reasonable doubt.*

In mathematics we use the second meaning: a proof establishes the incontrovertible *truth* of some assertion. To see what we mean, consider a simple claim (mathematicians use the word *theorem*).

Theorem 1.1. *The sum of any pair of even integers is even.*

Hopefully you believe this statement. But how do we *prove* it? We can *test* it by verifying examples ($4+6=10$ is even, $(-8)+30=22$ is even, etc.), but we cannot expect to verify *all* pairs this way. For a mathematical proof, we somehow need to test all possible examples simultaneously. To do this, it is essential that we have a clear idea of what is meant by an *even integer.*

Definition 1.2. An integer is *even* if it may be written in the form $2k$ where k is an integer.

Proof. Let x and y be even. Then $x=2k$ and $y=2l$ for some integers k and l. But then

$$x+y=2k+2l=2(k+l) \tag{$*$}$$

is even. ■

The box ■ indicates that we've finished our argument. Traditionally the letters Q.E.D. were used, an acronym for the Latin *quod erat demonstrandum* (*which is what was to be demonstrated*).

Consider how the proof depends crucially on the definition.

- The theorem did not mention any *variables,* though these were essential to the proof. The variables k and l come for free *once you write the definition of evenness!* This is very common; a proof is often little more than rearranged definitions.
- According to the definition, $2k$ and $2l$ together represent *all possible pairs* of even integers. It is essential that k and l be *different symbols,* otherwise all you would be proving is that twice an even number is even!
- The calculation $(*)$ is the easy bit; without the surrounding sentences and the direct reference to the definition of evenness, the calculation means nothing.

There is some sleight of hand here; a mathematical proof establishes truth only by reference to one or more definitions. In this case, the definition and theorem also depend on the meanings of *integer* and *sum,* but we haven't rigorously defined either since to do so would take us too far afield. In any context, some concepts will be considered too basic to merit definition.

Theorems & Conjectures

Theorems are true mathematical statements that we can prove. Some are important enough to be named (the Pythagorean theorem, the fundamental theorem of calculus, the rank–nullity theorem, etc.), but most are simple statements such as Theorem 1.1.

In practice we are often confronted with *conjectures*: statements we suspect to be true, but which we don't (yet) know how to prove. Much of the fun and messy creativity of mathematics lies in formulating and attempting to prove (or disprove) conjectures.

A conjecture is the mathematician's equivalent to the scientist's hypothesis: a statement one would like to be true. The difference in approach takes us right back to the dual meaning of *proof*. The scientist *tests* their hypothesis using the scientific method, conducting experiments which attempt (and hopefully fail!) to show that the hypothesis is incorrect. The mathematician tries to *prove* that a conjecture is undeniably true by relying on logic. The job of a mathematical researcher is to formulate conjectures, prove them, and publish the resulting theorems. Creativity lies as much in the formulation as in the proof. Attempting to formulate your own conjectures is an essential part of learning mathematics; many will likely be false, but you'll learn a lot in the process!

Here are two conjectures to give us a taste of this process.

Conjecture 1.3. *If n is any odd integer, then $n^2 - 1$ is a multiple of 8.*

Conjecture 1.4. *If n is any positive integer, then $n^2 + n + 41$ is prime.*[1]

How can we decide if these conjectures are true or false? To get a feel for things, we start by computing with several small integers n. In practice, this process is likely what lead to the formulation of the conjectures in the first place!

n	1	3	5	7	9	11	13
$n^2 - 1$	0	8	24	48	80	120	168

n	1	2	3	4	5	6	7
$n^2 + n + 41$	43	47	53	61	71	83	97

Since 0, 8, 24, 48, 80, 120 and 168 are all multiples of 8, and 43, 47, 53, 61, 71, 83 and 97 are all prime, both conjectures *appear* to be true. Would you bet \$100 that this is indeed the case? Is $n^2 - 1$ a multiple of 8 *for every* odd integer n? Is $n^2 + n + 41$ prime *for every* positive integer n? Establishing whether each conjecture is true or false requires one of the following:

Prove it by showing it must be true in <u>all</u> cases, or,

Disprove it by finding <u>at least one</u> instance in which the statement is false.

Let us start with Conjecture 1.3. If n is an odd integer, then, by definition, we may write $n = 2k + 1$ for some integer k. Now compute the object of interest:

$$n^2 - 1 = (2k+1)^2 - 1 = (4k^2 + 4k + 1) - 1 = 4k^2 + 4k = 4k(k+1)$$

We need to investigate whether this is *always* a multiple of 8. Since k is an integer, $n^2 - 1$ is plainly a multiple of 4, so everything comes down to deciding whether $k(k+1)$ is *always even.* Do we believe

[1] A positive integer is *prime* if it cannot be written as the product of two integers, both greater than one.

this? We return to testing some small values of k:

k	-2	-1	0	1	2	3	4
k^2+k	2	0	0	2	6	12	20

Once again, the claim seems to be true for small values of k, but how do we know it is true for *all* k? Again, the only way is to *prove* or *disprove it*. Observe that $k(k+1)$ is the *product of two consecutive integers.* This is great, because for any two consecutive integers, one is even and the other odd, so their product must be even. Conjecture 1.3 is indeed a *theorem!*

Everything so far has been investigative. Scratch work is an essential part of the process, but it isn't something we should expect a reader to have to fight their way through. We therefore offer a formal proof. This is the final result of our deliberations; investigate, spot a pattern, conjecture, prove, and finally present our work in as clean and convincing a manner as we can.

Theorem 1.5. *If n is any odd integer, then n^2-1 is a multiple of 8.*

Proof. Let n be any odd integer. By definition, we may write $n = 2k+1$ for some integer k. Then

$$n^2-1 = (2k+1)^2-1 = (4k^2+4k+1)-1 = 4k^2+4k = 4k(k+1)$$

We distinguish two cases. If k is even, then $k(k+1)$ is even and so $4k(k+1)$ is divisible by 8.

If k is odd, then $k+1$ is even. Therefore $k(k+1)$ is again even and $4k(k+1)$ divisible by 8.

In both cases $n^2-1 = 4k(k+1)$ is divisible by 8. ∎

All that work, just for five lines of clean argument! But wasn't it *fun*?

When constructing elementary proofs it is common to feel unsure over how much detail to supply. We plainly relied on the definition of *oddness*, but we also used the fact that a product is even whenever either factor is even; does this need a proof? Since the purpose of a proof is to convince the reader, the appropriateness of an argument will depend on context and your audience: if you are trying to convince a middle-school student, maybe you should justify this step more fully, though the cost would be a longer argument that might be harder to grasp in its totality. A perfect proof that is best for all situations is unlikely to exist! A good rule is to imagine you are writing for another mathematician at the same level as yourself—if a fellow student believes your argument, that's a good sign of its validity.

Now consider Conjecture 1.4. The question is whether n^2+n+41 is prime for *every* positive integer n. When $n \le 7$ the answer is yes, but examples do not make a proof! To investigate further, return to the definition of prime (Footnote 1): is there a positive integer n for which is n^2+n+41 can be factored as a product of two integers, both at least 2? A straightforward answer is staring us in the face! When $n = 41$ such a factorization certainly exists:

$$n^2+n+41 = 41^2+41+41 = 41(41+1+1) = 41 \cdot 43$$

We call $n = 41$ a *counterexample*; it shows that there is at least one integer n for which n^2+n+41 is *not* prime. Conjecture 1.4 is therefore false (it has been *disproved*).

Planning and Writing Proofs

Your main responsibility in this course is the construction of proofs. Their sheer variety means that, unlike in elementary calculus, you cannot simply practice computing tens of similar problems until the process becomes automatic. So how do you learn to write proofs?

The first step is to *read* other arguments. Don't just accept them, make sure you *believe* them: check the calculations, verify claims, rewrite the argument in your own words adding any clarification you think necessary.

As you read others' arguments, the question will often arise: *how did they ever come up with this?* As our work on Theorem 1.5 shows, the source of a proof is often less magical than it appears; usually the author experimented until they found something that worked. Most of that experimentation gets hidden in the final proof which should be as clean and easy to read as possible. Imagine it as a concert performance after lots of private practice; no-one wants to hear wrong notes at the Carnegie Hall!

In order to bridge the gap, we recommend splitting the proof-writing process into several steps.

Interpret Make sense of the statement. What is it saying? Can you rephrase in a way that is clearer to you? What are you assuming? The most important part of this step is identifying the *logical structure* of the statement. We'll discuss this at length in the next chapter.

Brainstorm Convince *yourself* that the statement is true. First, look up the relevant definitions. Next, think of some instances where the conditions of the statement are met. Try out some examples, and ask yourself what makes the claim work in those instances. Examples can be crucial for building intuition about *why* the claim is true and can sometimes suggest a proof strategy. Review other theorems that relate to these definitions. Do you know any theorems that relate your assumptions to the conclusion? Have you seen a proof of a similar statement before?

Sketch Build the skeleton of your proof. Think again about what you are assuming and what you are are you trying to prove. As we'll see in the next chapter, it is often straightforward to write down reasonable *first* and *last* steps (the bread slices of a *proof-sandwich*). Try to connect these with informal arguments. If you get stuck, try a different approach.

This step is often the longest in the proof-writing process. It is also where you will be doing most of your calculations. You can be as messy as you want because *no-one ever has to see it*! Once you've learned a variety of different proof methods, this is a good stage at which to experiment with different approaches.

Prove Once you have a suitable sketch, it's time to prove the statement to the world. Translate your sketch into a linear story, written in complete sentences. Carefully word your explanations and avoid shorthand, though well-understood mathematical symbols like $\Longrightarrow$ are encouraged. The result should be a clear, formal proof like you'd find in a mathematics textbook. Although you are providing a mathematical argument, your proof should read like prose.

Review Finally, *review* your proof. Assume the reader is meeting the problem for the first time and has not seen your sketch. Read your proof with skepticism; consider its readability and flow. Get read of unnecessary claims and revise the wording if necessary. Read your proof out loud. If you're adding extra words that aren't written down, include them in the proof. Finally, share your work with others. Do they understand it *without any additional input from you*?

Conjectures: *True* or *False*?

Higher-level mathematics is all about the important links between proofs, definitions, theorems and conjectures. We prove theorems (and solve homework problems) because they make us use, and aid our understanding of, definitions. We state definitions to help us formulate conjectures and prove theorems. One does not *know* mathematics, one *does* it. Mathematics is a *practice*; an art as much as it is a science.

With this in mind, do your best to prove or disprove the following conjectures. Don't worry if you're currently unsure as to the meanings of some of the terms or notation: ask! It will all be covered formally soon enough. At the end of the course, revisit these problems to realize how much your proof skills have improved.

1. The sum of any three consecutive integers is even.
2. There exist integers m and n such that $7m + 5n = 4$.
3. Every common multiple of 6 and 10 is divisible by 60.
4. There exist integers x and y such that $6x + 9y = 10$.
5. For every positive real number x, $x + \frac{1}{x}$ is greater than or equal to 2.
6. If x is any real number, then $x^2 \geq x$.
7. If n is any integer, $n^2 + 5n$ must be even.
8. If x is any real number, then $|x| \geq -x$.
9. If n is an integer greater than 2, then $n^2 - 1$ is not prime.
10. An integer is divisible by 5 when its last digit is 5.
11. If r is a rational number, then there is a non-zero integer n for which rn is an integer.
12. There is a smallest positive real number.
13. For all real numbers x, there exists a real number y for which $x < y$.
14. There exists a real number x such that, for all real numbers y, $x < y$.
15. The sets $A = \{n \in \mathbb{N} : n^2 < 25\}$ and $B = \{n^2 : n \in \mathbb{N} \text{ and } n < 5\}$ are equal. Here $\mathbb{N}$ denotes the set of natural numbers.

2 Logic and the Language of Proofs

2.1 Propositions

In order to read and construct proofs, we need to start with the language in which they are written: *logic*. This is to mathematics what grammar is to English.

Definition 2.1. A *proposition* or *statement* is a sentence that is either true or false.

Examples 2.2.
1. $17 - 24 = 7$.
2. 39^2 is an odd integer.
3. The moon is made of cheese.
4. Every cloud has a silver lining.
5. God exists.

For a proposition to make sense, we must agree on the meaning of each concept it contains. When people argue over propositions, in practice they are often disagreeing about *definitions*. There are many concepts of God; we cannot begin to consider whether or not They exist until we agree *which* concept is being discussed! This also illustrates that the truth status of a proposition *need not be known* at the moment you state it; this is particularly common in mathematics.[2]

Truth Tables and Combining Propositions

To develop basic rules and terminology, it is helpful to consider *abstract* propositions: $P, Q, R, \ldots$. Given a small number of propositions, all possible combinations of truth states may be easily represented in tabular format: in a *truth table*. These are useful for defining new propositions.

Definition 2.3. Let P and Q be propositions. The truth tables below define three new propositions modeled on the words *and*, *or* and *not*.

- The *conjunction* $P \wedge Q$ is read "P and Q."
- The *disjunction* $P \vee Q$ is read "P or Q."
- The *negation* $\neg P$ is read "not P."

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

P	$\neg P$
T	F
F	T

The letters T/F stand for *true/false*. E.g., the second line of the first table says that if P is true and Q is false, then the proposition "P and Q" is false, while "P or 'Q" is true.

Example 2.4. Suppose P and Q are the following propositions:

P: "I like purple." Q: "I like chartreuse."

We form the new propositions described in the definition:

$P \wedge Q$: "I like purple and chartreuse." $P \vee Q$: "I like purple or chartreuse."

$\neg P$: "I do not like purple."

It is typical to modify phrasing to aid readability: "Not, I like purple" just sounds weird! Note also that or is *inclusive* in logic: if "I like purple or chartreuse" is true, then you might like *both*!

[2]More surprisingly, there are even propositions whose truth state is impossible to determine!

Let's continue by adding a third proposition:

R: "It's 9am."

What proposition is represented by the following English sentence?

"I like purple and I like chartreuse or it's 9am."

Is it $P \wedge (Q \vee R)$ or is it $(P \wedge Q) \vee R$? Without brackets, the sentence is unclear; the moral is that English is terrible at logic! Indeed, as the truth table shows, the two logical expressions really do mean different things!

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$(P \wedge Q) \vee R$
T	T	T	T	T	T	T
T	T	F	T	T	T	T
T	F	T	T	T	F	T
T	F	F	F	F	F	F
F	T	T	T	F	F	T
F	T	F	T	F	F	F
F	F	T	T	F	F	T
F	F	F	F	F	F	F

Conditional and Biconditional Connectives

Of critical importance is the ability to have one proposition lead to another.

Definition 2.5. Given propositions P, Q, the *conditional* ($\Longrightarrow$) and *biconditional* ($\Longleftrightarrow$) *connectives* define new propositions as described in the truth table.

For the proposition $P \Longrightarrow Q$, we call P the *hypothesis* and Q the *conclusion*.

P	Q	$P \Longrightarrow Q$	$P \Longleftrightarrow Q$
T	T	T	T
T	F	F	F
F	T	T	F
F	F	T	T

Connective propositions can be read and written in many different ways:

$P \Longrightarrow Q$		$P \Longleftrightarrow Q$
P implies Q	P therefore Q	P if and only if Q
If P, then Q	Q follows from P	P iff Q
P only if Q	Q if P	P and Q are (logically) equivalent
P is sufficient for Q	Q is necessary for P	P is necessary and sufficient for Q

Example 2.6. The following sentences express, in English, the same conditional $P \Longrightarrow Q$.

- If you are born in Rome, then you are Italian.
- You are Italian if you are born in Rome.
- You are born in Rome only if you are Italian.
- Being born in Rome is sufficient for being Italian.
- Being Italian is necessary for being born in Rome.

Are you comfortable with what the propositions P and Q are here?

Connectives are central to mathematics for many reasons. In particular:

1. The vast majority of theorems we'll encounter may be written as a connective $P \implies Q$. For instance, revisit Theorem 1.1 and the discussion that follows:

   If x and y are even integers, then $x + y$ is even.

   Identifying the hypothesis and conclusion is essential if you want to understand a theorem!

2. Simple proofs typically involve chaining a sequence of connectives:

   $$P \implies P_2 \implies \cdots \implies P_n \implies Q$$

We'll revisit these ideas in Section 2.3, and repeatedly throughout the course.

While the biconditional should be easy to remember, it is harder to make sense of the conditional connective. Short of simply memorizing the truth table, here are two examples that might help.

Examples 2.7. 1. Suppose your professor says, "If the class earns a B average on the midterm, then I'll bring doughnuts." The only situation in which the teacher will have lied is if the class earns a B average but she fails to provide doughnuts.

2. ($F \implies T$ really can be true!) Let P be the proposition "$7 = 3$" and Q be "$0 = 0$." Since multiplication of both sides of an equation by zero is algebraically valid, we see that

   $$\begin{aligned} 7 = 3 &\implies 0 \cdot 7 = 0 \cdot 3 && \text{(If } 7 = 3\text{, then 0 times 7 equals 0 times 3)} \\ &\implies 0 = 0 && \text{(then 0 equals 0)} \end{aligned}$$

   This argument is perfectly correct: the *implication* $P \implies Q$ is *true.* It (rightly!) makes us uncomfortable because the hypothesis is *false.*

   If we instead add 1 to each side of $7 = 3$, we'd obtain a example where $F \implies F$ is true.

Tautologies and Contradictions

Definition 2.8. A *tautology* is a logical expression that is always true, regardless of what the component statements might be.
A *contradiction* is a logical expression that is always false.

Examples 2.9. 1. $P \wedge (\neg P)$ is a contradiction.

Regardless of the proposition P, it cannot be true at the same time as its negation!

P	$\neg P$	$P \wedge (\neg P)$
T	F	F
F	T	F

2. $\big(P \wedge (P \implies Q)\big) \implies Q$ is a tautology.

P	Q	$P \implies Q$	$P \wedge (P \implies Q)$	$\big(P \wedge (P \implies Q)\big) \implies Q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

The Converse and Contrapositive

Definition 2.10. The *converse* of $P \implies Q$ is the reversed implication $Q \implies P$.
The *contrapositive* of $P \implies Q$ is the implication $\neg Q \implies \neg P$.

It is vital to understand the distinction between these. In general, the truth status of the converse bears no relation to that of the original, though the contrapositive is much better behaved.

Theorem 2.11. *The contrapositive of an implication is logically equivalent to the original.*

Proof. Compute the truth table and observe that the third and sixth columns are identical:[3]

P	Q	$P \implies Q$	$\neg Q$	$\neg P$	$\neg Q \implies \neg P$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

∎

Example 2.12. Let P and Q be the following statements:

P: "Claudia is holding a peach." Q: "Claudia is holding a piece of fruit."

Since a peach is indeed a piece of fruit, the proposition $P \implies Q$ is *true*:

$P \implies Q$: "If Claudia is holding a peach, then she is holding a piece of fruit."

The *converse* of $P \implies Q$ is the sentence

$Q \implies P$: "If Claudia is holding a piece of fruit, then she is holding a peach."

This is palpably false: Claudia could be holding an apple! However, in accordance with Theorem 2.11, the *contrapositive* is *true*:

$\neg Q \implies \neg P$: "If Claudia is *not* holding any fruit, then she is *not* holding a peach."

Negating Logical Expressions

Mathematics often requires us to negate propositions. What would you suspect to be the negation of a conditional $P \implies Q$? Is it enough to say "P doesn't imply Q"? But what does this mean?

We again rely on a truth table: to get the last column, recall that negation simply swaps T and F. Can we write this column in another way? Since there is only a single T in the final column, we see that we've proved the following.

P	Q	$P \implies Q$	$\neg(P \implies Q)$
T	T	T	F
T	F	F	T
F	T	T	F
F	F	T	F

Theorem 2.13. $\neg(P \implies Q)$ *is logically equivalent to* $P \wedge \neg Q$ *("P and not Q").*

[3]Otherwise said, $(P \implies Q) \iff (\neg Q \implies \neg P)$ is a tautology.

Example 2.14. Consider the implication

> It's the morning therefore I'll have coffee.

Hopefully its negation is clear:

> It's the morning *and* I *won't* have coffee.

As in Example 2.7, it might help to think about what it means for the original statement to be *false*.

Warning! The negation of $P \implies Q$ is *not a conditional.* In particular it is *neither* of the following:

> The converse $Q \implies P$.
>
> The contrapositive of the converse $\neg P \implies \neg Q$.

If you are unsure about this, write down the truth tables and compare.

Our final results in basic logic also involve negations; they are named for Augustus de Morgan, a famous 19^{th} century logician.

Theorem 2.15 (de Morgan's laws). *Let P and Q be propositions.*

1. $\neg(P \wedge Q)$ *is logically equivalent to* $\neg P \vee \neg Q$
2. $\neg(P \vee Q)$ *is logically equivalent to* $\neg P \wedge \neg Q$

Proof. For the first law, observe that the fourth and seventh columns of the truth table are identical.

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

The second law is an exercise. ■

Example 2.16. Consider the sentence:

> I rode the subway *and* I had coffee.

To negate this using de Morgan's first law, we might write:

> I *didn't* ride the subway *or* I *didn't* have coffee.

Subway	Coffee	Su and Co
T	T	T
T	F	F
F	T	F
F	F	F

This feels awkward in English because the negation encompasses three distinct possibilities. Note how the logical (inclusive) use of *or* includes the last row of the truth table: the possibility that you neither rode the subway nor had coffee.

As with Example 2.4, this is another advert for the use of logic: English simply isn't very helpful for precisely stating complex logical statements.

Aside: Algebraic Logic We can use truth tables to establish other laws of basic logic, for instance:

Double negation	$\neg(\neg P) \iff P$	
Commutativity	$P \wedge Q \iff Q \wedge P$	$P \vee Q \iff Q \vee P$
Associativity	$(P \wedge Q) \wedge R \iff P \wedge (Q \wedge R)$	$(P \vee Q) \vee R \iff P \vee (Q \vee R)$
Distributivity	$(P \wedge Q) \vee R \iff (P \vee R) \wedge (Q \vee R)$	$(P \vee Q) \wedge R \iff (P \wedge R) \vee (Q \wedge R)$

To make things more algebraic, we've replaced "is logically equivalent to" with a biconditional.[4]

Armed with such laws, one can often suitably manipulate logical expressions without laboriously creating truth tables. This is not the focus of this course, though you might find it fun!

For this course, it is probably not worth memorizing these laws. Your intuitive understanding of *and*, *or* and *not* mean you'll likely apply the laws correctly whenever necessary.

Exercises 2.1. A reading quiz and several questions with linked video solutions can be found online.

1. Express each statement in the form, "If . . . , then . . . " There are many possible correct answers.
   (a) You must eat your dinner if you want to grow.
   (b) Being a multiple of 12 is a sufficient condition for a number to be even.
   (c) It is necessary for you to pass your exams in order for you to obtain a degree.
   (d) A triangle is equilateral only if all its sides have the same length.

2. Suppose "x is an even integer" and "y is an irrational number" are true statements, and that "$z \geq 3$" is a false statement. Which of the following are true?

   (*Hint: Label each statement and think about each using connectives*)

   (a) If x is an even integer, then $z \geq 3$.
   (b) If $z \geq 3$, then y is an irrational number.
   (c) If $z \geq 3$ or x is an even integer, then y is an irrational number.
   (d) If y is an irrational number and x is an even integer, then $z \geq 3$.

3. Orange County is considering two competing transport plans: widening the 405 freeway and constructing light rail down its median. A local politician is asked, "Would you like to see the 405 widened or would you like to see light rail?" The politician wants to sound positive, but to avoid being tied to one project. What is their response?

   (*Hint: Think about how the word 'OR' is used in logic*)

4. Consider the proposition: "If the integer m is greater than 3, then $2m$ is not prime."
   (a) Rewrite the proposition using the word 'necessary.'
   (b) Rewrite the proposition using the word 'sufficient.'
   (c) Write the negation, converse and contrapositive of the proposition.

5. Suppose the following sentence is true: "If Amy likes art, then no-one likes history." What, if anything, can we conclude if we discover that someone likes history.

[4] Stating the laws in this fashion is to assert that each expression is a tautology (Definition 2.8). For instance, to claim that "$\neg(\neg P)$ is logically equivalent to P" is to assert that $\neg(\neg P) \iff P$ is a tautology.

6. Construct the truth tables for the propositions $P \vee (Q \wedge R)$ and $(P \vee Q) \wedge R$. Are they the same?
7. Use truth tables to establish the following laws of logic:
   (a) Double negation: $\neg(\neg P) \iff P$.
   (b) Idempotent law: $P \wedge P \iff P$.
   (c) Absorption law: $P \wedge (P \vee Q) \iff P$.
   (d) Distributive law: $(P \wedge Q) \vee R \iff (P \vee R) \wedge (Q \vee R)$.
8. (a) Decide whether $(P \wedge \neg P) \implies Q$ is a tautology, a contradiction, or neither.
   (b) Explain why $\neg P \vee \neg Q$ is logically equivalent to $P \implies (P \wedge \neg Q)$.
   (c) Prove: $\big((P \wedge \neg Q) \implies F\big) \iff (P \implies Q)$ is a tautology. Here F represents a *contradiction.*
9. (a) Prove that the expressions $(P \implies Q) \wedge (Q \implies P)$ and $P \iff Q$ are logically equivalent.
   (b) Prove that $\big((P \implies Q) \wedge (Q \implies R)\big) \implies \big(P \implies R\big)$ is a tautology.

   Why do these make intuitive sense?
10. Use logical algebra (e.g., page 11) to show that $\big((P \vee Q) \wedge \neg P\big) \wedge \neg Q$ is a contradiction.
11. Do there exist propositions P, Q for which both $P \implies Q$ and its converse are *false*? Explain.
12. Your friend insists that the negation of the sentence "Mark and Mary have the same height" is "Mark or Mary do not have the same height." What is the correct negation? Where did your friend go wrong?
13. Suppose that the following statements are *true*:
    (a) Every octagon is magical.
    (b) If a polygon is not a rectangle, then is it not a square.
    (c) A polygon is a square, if it is magical.

    Is it true that "Octagons are rectangles"? Explain your answer.

    (*Hint: try rewriting each of the statements as an implication*)
14. The connective $\downarrow$ (the *Quine dagger*, *NOR*) is defined by the truth table:

P	Q	$P \downarrow Q$
T	T	F
T	F	F
F	T	F
F	F	T

    (a) Prove that $P \downarrow Q$ is logically equivalent to $\neg(P \vee Q)$.
    (b) Find a logical expression built using only P and the connective $\downarrow$ which is logically equivalent to $\neg P$.
    (c) Find an expression built using only P, Q and $\downarrow$ which is logically equivalent to $P \wedge Q$.
15. (Just for fun) Augustus de Morgan satisfied his own problem:

    I turn(ed) x years of age in the year x^2.

    (a) Given that de Morgan died in 1871, and that he wasn't the beneficiary of some miraculous anti-aging treatment, find the year in which he was born.
    (b) Suppose you have an acquaintance who satisfies the same problem. When were they born and how old will they turn this year?

Do your best to give a formal proof of your correctness.

2.2 Propositional Functions & Quantifiers

The majority of mathematical propositions are more complicated that those seen in Section 2.1. In particular, they typically involve *variables*, for instance

> "x is an integer greater than 5."

Definition 2.17. A *propositional function* is a family of propositions which depend on one or more variables. The collection of permitted variables is the *domain*.

If P is a propositional function depending on a single variable x, then for each object a in the domain, $P(a)$ is a proposition. Typically $P(x)$ is true for some x and false for others.

Example 2.18. Consider the propositional function $P(x)$: "$x^2 > 4$" with domain the real numbers. Plainly $P(1)$ is false ("$1^2 > 4$") and $P(6)$ is true ("$6^2 > 4$").

In mathematics, propositional functions are often *quantified*. English contains various quantifiers (*all, some, many, few, several*, etc.), but in mathematics we are primarily concerned with just two.

Definition 2.19. The *universal quantifier* $\forall$ is read 'for all'. The *existential quantifier* $\exists$ is read 'there exists.' Given a propositional function $P(x)$, we define two new *quantified propositions*:

- "$\forall x, P(x)$" is true if and only if $P(x)$ is true for *every* x in its domain.
- "$\exists x, P(x)$" is true if and only if $P(x)$ is true for *at least one* x in its domain.

It is common to describe the domain when quantifying propositions by including a descriptor after the quantifier (*bounding the quantifier*—see below).

As with connectives, there are many ways to express quantified propositions both mathematically and in English. The use of symbolic quantifiers involves a trade-off: compact statements can improve clarity, but they are harder to read for the uninitiated, so consider your audience! While it is your choice whether to employ symbolic quantifiers in your own *writing*, it is essential that you know how to *read/recognize* them and that you can *translate* between various incarnations.

Example (2.18 cont.). To gain some practice with bounded quantifiers, we introduce the notation $x \in \mathbb{R}$: this means that x is a real number.

- "$\forall x \in \mathbb{R},\ x^2 > 4$" might be read, "The square of every real number is greater than 4."

  The quantified expression is *false* since $1^2 > 4$ is false: we call $x = 1$ a *counter-example*.
- "$\exists x \in \mathbb{R},\ x^2 > 4$" might be read, "There is a real number whose square is greater than 4."

  The quantified expression is *true* since $6^2 > 4$ (is true): we call $x = 6$ an *example*.

Due to their importance, it is worth defining these last concepts formally.

Definition 2.20. An *example* of $\exists x, P(x)$ is an element x_0 in the domain of P for which $P(x_0)$ is *true*. A *counter-example* to $\forall x, P(x)$ is an element x_0 in the domain of P for which $P(x_0)$ is *false*.

Universal Quantifiers and Connectives: Hidden Quantifiers Universally quantified statements are interchangeable with implications. Given a propositional function $Q(x)$, let $P(x)$ be the proposition "x lies in the domain of Q." Then

$$\boxed{\forall x, Q(x) \text{ is logically equivalent to } P(x) \implies Q(x)}$$

Connectives containing variables are therefore assumed to be universal. When written as a connective, the universal quantifier is typically *hidden*.[5]

Examples 2.21. 1. The universal statement "Every cat is neurotic," may also be written

If x is a cat, then x is neurotic.

2. Revisiting Example 2.18, we could rewrite "$\forall x \in \mathbb{R}, x^2 > 4$" as a connective

$$x \in \mathbb{R} \implies x^2 > 4 \qquad \text{(If } x \text{ is a real number, then } x^2 > 4\text{)}$$

3. The following three sentences have identical meaning:

The square of an odd integer is odd. $\quad \forall n$ odd, n^2 is odd. $\quad n$ odd $\implies n^2$ odd.

In only one of the sentences is the universal quantifier explicit. For even more variety, the third sentence can also be viewed as a universal statement about all *integers*; including the hidden quantifier in this case results in

$$\forall n \in \mathbb{Z},\ n \text{ odd} \implies n^2 \text{ odd}.$$

where the symbol $\mathbb{Z}$ represents the (set of) integers.

We've already seen that *disproving* a universal statement requires only that we supply a *counter-example.* While such might require some effort to find, often the resulting argument is very simple. By contrast, *proving* a universal statement is the same as proving a connective, an activity that is typically much more involved. We therefore largely postpone this to the next section. Regardless, a simple proof of our *oddness* claim should be easy to follow.

Proof of Example 2.21.3. If an integer n is odd, then it may be written in the form $n = 2k + 1$ for some integer k. But then

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

is plainly also odd. ∎

Similarly, *proving* an existential statement (by providing an *example*) is typically more straightforward than *disproving* such. To understand this duality, we need to understand how to *negate* quantified propositions.

[5] By contrast, the existential quantifier is never hidden: it is always explicitly written as a symbol ($\exists$), or as a phrase in English (*there is, there exists, some, at least one,* etc.).

Negating Quantified Propositions

To negate a proposition, we consider what it means for it to be *false*. We already understand what this means for a universal proposition:

"$\forall x, P(x)$" is false if and only if *there exists a counter-example.*

The negation of a universal statement is *existentially quantified*:

The negation of "$P(x)$ is *always* true" is "$P(x)$ is *sometimes* false."

Repeating this with $\neg P(x)$ results in a related observation:

The negation of "$P(x)$ is *always* false" is "$P(x)$ is *sometimes* true."

Theorem 2.22. *For any propositional function $P(x)$:*

1. $\neg(\forall x, P(x))$ *is logically equivalent to* $\exists x, \neg P(x)$.
2. $\neg(\exists x, P(x))$ *is logically equivalent to* $\forall x, \neg P(x)$.

Examples 2.23. 1. "Everyone owns a bicycle," has negation, "Someone does not own a bicycle." It is somewhat ugly, but we could write this symbolically:

$$\neg(\forall \text{ people } x,\ x \text{ owns a bicycle}) \iff \exists \text{ a person } x \text{ such that } x \text{ does not own a bicycle}$$

2. The quantified proposition[6] "$\exists x > 0$ such that $\sin x = 4$," has the form $\exists x,\ P(x)$. Its negation has the form $\forall x,\ \neg P(x)$. Explicitly:

$$\forall x > 0,\ \sin x \neq 4$$

Since the sine function satisfies the inequalities $-1 \leq \sin x \leq 1$, the original proposition is *false* and its negation *true*.

Warning! *Never* negate a quantifier's bounds: $\forall x \leq 0 \ldots$ is completely wrong!

3. Be especially careful when negating connectives: after negation, a hidden quantifier $\forall x$ becomes *explicit*.

$$\neg\big(P(x) \implies Q(x)\big) \text{ is logically equivalent to } \exists x, P(x) \wedge \neg Q(x)$$

(a) (Example 2.21.3) The negation of "n odd $\implies n^2$ odd"is the (false) claim

$\exists n \in \mathbb{Z}$ with n odd *and* n^2 even.

(b) (Example 2.18) The negation of the false claim "$x \in \mathbb{R} \implies x^2 > 4$" is the true assertion

$\exists n \in \mathbb{R}$ for which $x^2 \leq 4$

[6] "$\exists x > 0$" indicates that the domain of the proposition "$\sin x = 4$" is the *positive* real numbers.

Multiple Quantifiers

A propositional function can have several variables, each of which may be quantified.

Examples 2.24. 1. The quantified proposition

$$\forall x > 0, \exists y > 0 \text{ such that } xy = 4$$

might be read, "Given any positive number, there is another such that their *product* is four." Hopefully you believe that this is *true*! Here is a simple argument which comes from viewing it as an implication, "If $x > 0$, then $\exists y > 0$ such that $xy = 4$."

Proof. Suppose we are given $x > 0$. Let $y = \frac{4}{x}$, then $xy = 4$, as required. ∎

Being clear about *domains* is critical. Suppose we modify the original proposition:

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R} \text{ such that } xy = 4 \tag{†}$$

Our proof now fails! The new statement (†) is *false*: indeed $x = 0$ provides a *counter-example.*

Disproof. Let $x = 0$. Since $xy = 0$ for any real number y, we cannot have $xy = 4$. ∎

Alternatively, we could *negate* (†): following Theorem 2.22, we switch the symbols $\forall \leftrightarrow \exists$ and negate the final proposition,[7]

$$\neg\big(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, xy = 4\big) \iff \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \ xy \neq 4 \tag{¬(†)}$$

Our *disproof* of (†) is really a *proof* of the negation: we provided the *example* $x = 0$, thus demonstrating the truth of a $\exists$-statement. Since the negation is true, the original (†) is false.

2. Order of quantifiers matters! The meaning of a sentence will likely change if we alter the order of quantification. This might also change the truth state of a proposition.

   (a) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^2 < y$

   Proof. Suppose a real number x is given. Let $y = x^2 + 1$, then $x^2 < y$, as required. ∎

   We proved this by viewing it as an implication, "If $x \in \mathbb{R}$, then $\exists y \in \mathbb{R}, x^2 < y$."

   (b) $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, x^2 < y$

   Disproof. We demonstrate the truth of the negation, "$\forall y, \exists x, x^2 \geq y$."
   Suppose a real number y is given. Let $x = \sqrt{|y|}$, then $x^2 = y \geq y$, as required. ∎

---

[7] Here is an abstract justification for this heuristic. Consider a propositional function $P(x)$: "$\exists y, Q(x,y)$," then

$$\begin{aligned} \neg(\forall x, \exists y, Q(x,y)) &\iff \neg(\forall x, P(x)) \iff \exists x, \neg P(x) \iff \exists x, \neg(\exists y, Q(x,y)) \\ &\iff \exists x, \forall y, \neg Q(x,y) \end{aligned}$$

Putting it all together We finish with two examples you might have seen elsewhere. For this course, *you do not have to know what these statements mean,* though you do have to be able to *negate* them.

Examples 2.25. 1. Vectors $\mathbf{x}, \mathbf{y}, \mathbf{z}$ in the vector space $\mathbb{R}^3$ are *linearly independent* if

$$\forall a, b, c \in \mathbb{R},\ a\mathbf{x} + b\mathbf{y} + c\mathbf{z} = \mathbf{0} \implies a = b = c = 0$$

In a linear algebra course, the expression $\forall a, b, c \in \mathbb{R}$ would often be hidden. The negation of this statement, what it means for $\mathbf{x}, \mathbf{y}, \mathbf{z}$ to be *linearly dependent,* is

$$\exists a, b, c \in \mathbb{R},\ \text{not all zero, such that } a\mathbf{x} + b\mathbf{y} + c\mathbf{z} = \mathbf{0}$$

2. A function $f : \mathbb{R} \to \mathbb{R}$ is said to be *continuous at* $a \in \mathbb{R}$ if

$$\forall \epsilon > 0,\ \exists \delta > 0 \text{ such that } |x - a| < \delta \implies |f(x) - f(a)| < \epsilon$$

The negation, what it means for f to be *discontinuous at* $x = a$, is

$$\exists \epsilon > 0 \text{ such that } \forall \delta > 0,\ \exists x \in \mathbb{R} \text{ with } |x - a| < \delta \text{ and } |f(x) - f(a)| \geq \epsilon$$

The original statement contained a hidden quantifier $\forall x$ which became explicit upon negation.

Exercises 2.2. A self-test quiz and several worked questions can be found online.

1. Rewrite each sentence using quantifiers. Then write the negation (use words and quantifiers).
   (a) All mathematics exams are hard.
   (b) No football players are from San Diego.
   (c) There is a odd number that is a perfect square.
2. Let P be the proposition: "Every positive integer is divisible by thirteen."
   (a) Write P using quantifiers.
   (b) What is the negation of P?
   (c) Is P true or false? Prove your assertion.
3. A friend claims that the sentence "$x^2 > 0 \implies x > 0$" has negation "$x^2 > 0$ and $x \leq 0$." Why is this incorrect? What is the correct negation?
4. Consider the quantified statement
   $$\forall x, y, z \in \mathbb{R},\ (x-3)^2 + (y-2)^2 + (z-7)^2 > 0 \tag{$*$}$$
   (a) Express $(*)$ in words.
   (b) Is $(*)$ true or false? Explain.
   (c) Express the negation of $(*)$ in symbols, and then in words.
   (d) Is the negation of $(*)$ true or false? Explain.
5. Suppose P, Q, R are propositional functions. Compute the negations of the following:
   (a) $\forall x, \exists y, P(x) \wedge Q(y)$ (b) $\forall x, \exists y, \forall z, R(x, y, z)$

6. Revisit Example 2.24.2. Decide whether each of the following is true or false:
   (a) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x^2 < y$ (b) $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}, x^2 < y$
7. The following are statements about positive real numbers x, y. Which is true? Explain.
   (a) $\forall x$, $\exists y$ such that $xy < y^2$ (b) $\exists x$ such that $\forall y$, $xy < y^2$
8. Which of the following statements are true? Explain.
   (a) $\exists$ a married person x such that $\forall$ married people y, x is married to y.
   (b) $\forall$ married people x, $\exists$ a married person y such that x is married to y.
9. Prove or disprove the following statements.
   (a) For every two points A and B in the plane, there exists a circle on which both A and B lie.
   (b) There exists a circle in the plane on which lie any two points A and B.
10. Consider the following proposition (*you do not have to know what is meant by a field*).

    All non-zero elements x in a field $\mathbb{F}$ have an inverse: some $y \in \mathbb{F}$ for which $xy = 1$.

    (a) Restate the proposition using quantifiers.
    (b) Find the negation of the proposition, again using quantifiers.
11. A function $f : \mathbb{R} \to \mathbb{R}$ is said to be *decreasing* if:

    $$x \leq y \implies f(x) \geq f(y)$$

    (a) State what it means for f not to be decreasing (*where is the hidden quantifier?*)
    (b) Give an example to show that *not decreasing* and *increasing* do not mean the same thing.
12. Consider the proposition:

    $$\forall m, n \in \mathbb{R}, \quad m > n \implies m^2 > n^2$$

    (a) State the negation of the proposition.
    (b) Prove that the original proposition is *false*.
    (c) Suppose you rewrite the proposition:

    $$\forall m, n \in A, m > n \implies m^2 > n^2$$

    What is the largest collection (set) of real numbers A for which the proposition is *true*?
13. (Hard) Let $(x_n) = (x_1, x_2, x_3, \ldots)$ denote a sequence of real numbers.

    "(x_n) *diverges to* ∞" means: $\forall M > 0$, $\exists N \in \mathbb{R}$ such that $n > N \implies x_n > M$
    "(x_n) *converges to* L" means: $\forall \epsilon > 0$, $\exists N \in \mathbb{R}$ such that $n > N \implies |x_n - L| < \epsilon$

    (a) State what it means for a sequence (x_n) not to diverge to ∞. *Beware of the hidden quantifier!*
    (b) State what it means for a sequence (x_n) not to converge to L.
    (c) State what it means for a sequence (x_n) not to converge at all.
    (d) (Challenge: non-examinable) Use the definitions to prove that the sequence defined by $x_n = n$ diverges to ∞, and that the sequence defined by $y_n = \frac{1}{n}$ converges to zero.

2.3 Methods of Proof

Everything thus far has been in service to what follows: to provide the language and logical fluency necessary to understand mathematical arguments and to begin to create your own. One can study foundational logic much more deeply, but that is not our purpose. The real work begins now.

In mathematics, a Theorem is[8] a justified assertion of the truth of an implication $P \implies Q$. A *proof*, for there can be many different approaches, is any logical argument which justifies the theorem. The first step in analyzing or strategizing a proof is to identify the hypothesis P and conclusion Q.

There are four standard methods of proof, though a longer argument might use several.

Direct Assume the hypothesis P and deduce the conclusion Q.[9] This structure should be intuitive, though it may help to revisit the truth table in Definition 2.5 and the tautology of Example 2.9.2.

Contrapositive Assume $\neg Q$ and deduce $\neg P$: a direct proof of the contrapositive $\neg Q \implies \neg P$. This approach works because the contrapositive is logically equivalent to $P \implies Q$ (Theorem 2.11).

Contradiction Assume P and $\neg Q$, and deduce a *contradiction*. By Theorem 2.13 and Exercise 2.1.8c, we see that $P \implies Q$ is true.

Induction This has a completely different flavor: we will consider it in Chapter 5.

Each method has its advantages and disadvantages: the direct method typically has a simpler logical flow whereas the contrapositive/contradiction approaches are useful when the negations $\neg P$, $\neg Q$ are easier to work with than P, Q themselves. All methods are equally valid, and, as we'll see shortly, one can often prove a simple theorem using all three approaches!

As you work through this section, pay special attention to the logical structure—to encourage this, the mathematical level of this section is very low—and refer to the previous sections if the logical terminology feels unfamiliar. In particular, re-read *Planning and Writing Proofs* (page 4).

Direct Proofs

We begin by generalizing Example 2.21.3.

Theorem 2.26. *The product of any pair of odd integers is odd.*

To make sense of this, we first need to identify the logical structure by writing the theorem in terms of propositions and connectives. One way is to view the Theorem in the form $P(x,y) \implies Q(x,y)$:

- $P(x,y)$ is "x and y are both odd." This is our assumption, the hypothesis.
- $Q(x,y)$ is "The product of x and y is odd." This is what we wish to demonstrate, the conclusion.
- Both propositional functions are statements about *integers.* The Theorem is *universal* ("any pair"), and so contains a (hidden) quantifier $\forall x, y \in \mathbb{Z}$.

To perform a proof, we also need a clear understanding of the meaning of all necessary terms. To keep things simple, we'll take *integer* and *product* as understood and be explicit as to the meaning of *oddness.*

[8] It is sometimes awkward to fit a theorem into this format but it can always be done. Often all that is stated is the conclusion Q, in which case P would be the assertion "All mathematics we already know/assume to be true."

[9] From now on, to *assume* a proposition is to suppose its *truth.* To suppose P is false, we "assume/suppose $\neg P$."

A direct proof can be viewed as a proof sandwich, whose bread slices are the hypothesis and conclusion (P and Q): write these down as a first step. Next define any useful terms in the hypothesis. All that remains is to perform a simple calculation!

Proof. Let x and y be odd integers. (state hypothesis P)
There are integers k, l for which $x = 2k+1$ and $y = 2l+1$. Then, (definition of *odd*)

$$\begin{aligned} xy &= (2k+1)(2l+1) = 4kl + 2k + 2l + 1 \\ &= 2(2kl + k + l) + 1 \end{aligned} \qquad \text{(computation/algebra)}$$

Since $2kl + k + l$ is an integer, we conclude that xy is odd. ∎ (state conclusion Q)

To make the conclusion absolutely clear, we explicitly wrote xy in the form 2(integer)+1.

Insufficient Generality Before leaving this example, it is worth quickly highlighting the most common mistakes seen in such arguments.

Fake Proof 1. $x = 3$ and $y = 5$ are both odd, hence $xy = 15$ is odd.

This is an *example* of the theorem. Since the theorem is *universal,* a single example is not a proof.

Fake Proof 2. Let $x = 2k+1$ and $y = 2k+1$ be odd. Then

$$xy = (2k+1)(2k+1) = 2(2k^2 + 2k) + 1 \quad \text{is odd.}$$

This is still insufficiently general in that it only verifies a special case (x odd $\implies x^2$ odd). There is nothing wrong with trying out examples or sketching incomplete thoughts—indeed both are encouraged!—but you need to be aware of when your argument isn't sufficiently general.

For another simple direct proof, consider the sum of two consecutive integers.

Theorem 2.27. *The sum of any pair consecutive integers is odd.*

The theorem is again a universal claim of the form $P(x,y) \implies Q(x,y)$ about two integers:

- $P(x,y)$ is "x, y are consecutive integers."
- $Q(x,y)$ is "$x + y$ is odd."

The trick is to observe that, being consecutive, we may write y in terms of x. The proof sandwich is still visible, though it would be hard to write down the last sentence without already having settled on the trick, which is essentially the definition of "consecutive integers."

Proof. Suppose we are given two consecutive integers. Label the smaller of these x, then the other $x+1$. But then their sum

$$x + (x+1) = 2x + 1$$

is odd. ∎

Proof by Contrapositive

Here is another simple result about odd and even integers.

Theorem 2.28. *If the sum of two integers is odd, then they have opposite parity.*

The theorem is yet another universal statement ($\forall x, y \in \mathbb{Z}$) of the form $P(x,y) \implies Q(x,y)$:

$P(x,y)$: "$x+y$ is odd." $\qquad$ $Q(x,y)$: "x, y have opposite parity."

Parity means *evenness or oddness*: the conclusion is that one of x, y is even and the other odd.

Attempting a direct proof results in an immediate difficulty:

Direct Proof? Suppose $x+y$ is odd. Then $x+y = 2k+1$ for some integer k...

We want to conclude something about x and y *individually*, but the direct approach lumps them together in the same algebraic expression.

A contrapositive argument suggests itself because the new hypothesis $\neg Q$, in treating x and y separately, gives us twice as much to start with.[10]

$\neg Q(x,y)$: "x, y have the same parity." $\qquad$ $\neg P(x,y)$: "$x+y$ is even."

The minor remaining difficulty is that "same parity" encompasses *two* possibilities: x, y are either both even, or both odd. The proof therefore contains two cases.

Proof. Suppose x and y have the same parity. There are two cases. (state hypothesis $\neg Q$)

Case 1: Assume x and y are both even.
 Write $x = 2k$ and $y = 2l$, for some integers k, l. (definition of *even*)
 Then $x+y = 2(k+l)$ is even. (computation)

Case 2: Assume x and y are both odd.
 Write $x = 2k+1$ and $y = 2l+1$ for some integers k, l. (definition of *odd*)
 Then $x+y = 2(k+l+1)$ is even. (computation)

In both cases $x+y$ is even. (state conclusion $\neg P$) ∎

Again observe the proof sandwich and how the proof depending on little more than the definitions of even and odd.

When presenting a lengthier argument, consider orienting the reader by starting with the phrase, "We prove the contrapositive." In simple cases like the above this is unnecessary, since the logical structure should be completely clear without such assistance. It is also unnecessary to define and spell out the propositions P and Q or include any of the bracketed commentary. However, you should feel free to continue this practice if you think it would aid your explanation, of if you are nervous about your proof skills.[11]

[10] Warning! The contrapositive is still a *universal* statement: $\forall x, y \in \mathbb{Z}, \neg Q(x,y) \implies \neg P(x,y)$. We are not negating the whole theorem so do not convert $\forall$ to $\exists$!

[11] ...and want to guarantee some partial credit!

For another example of a contrapositive argument, we extend the first result of this section.

Theorem 2.29. *The product of two integers is odd* if and only if *both integers are odd.*

This has the form $P \iff Q$, which comprises *two theorems in one*: $P \implies Q$ and $Q \implies P$ (see Exercise 2.1.9a). A contrapositive argument for the ($\Rightarrow$) direction is again suggested because the right hand side treats the two integers separately.

Proof. ($\Rightarrow$) We prove the contrapositive. Let x, y be integers, at least one of which is even. Suppose, *without loss of generality*, that $x = 2k$ is even. Then $xy = 2ky$ is also even.

($\Leftarrow$) This is precisely Theorem 2.26, which we've already proved. ∎

Without loss of generality Often abbreviated to WLOG, this phrase is common in mathematics. Here it saves us from performing the almost identical argument assuming $y = 2l$ is even. WLOG is stated when a mathematician makes a choice which does not materially affect the argument.

Proof by Contradiction

To introduce contradiction proofs consider another simple result.[12]

Example 2.30. Let x be an integer. If $3x + 5$ is even, then $5x + 2$ is odd.

We could proceed directly according to the following sketch:

$$3x + 5 \text{ even} \implies 3x \text{ odd} \implies x \text{ odd} \implies 5x \text{ odd} \implies 5x + 2 \text{ odd} \tag{$*$}$$

This isn't wrong! You should believe each implication; indeed we've proved most of them. However it would be nice not to rely on so many other results. A similar contrapositive approach (reverse arrows and negate propositions in ($*$)) would have the same weakness.

The advantage of a contradiction approach is that we have twice as much to work with: the hypothesis ($3x + 5$ even) *and* the negation of the conclusion ($5x + 2$ even).

Proof. Suppose both $3x + 5$ and $5x + 2$ are even. Then their sum is also even. However,

$$(3x + 5) + (5x + 2) = 8x + 7 = 2(4x + 3) + 1 \tag{$\dagger$}$$

is odd. Contradiction (an integer cannot be both even and odd!). ∎

Remember to mention the word *contradiction* at the end, so the reader knows what you've done.

A nice side-effect of this approach is that it suggests an alternative *direct proof.*

Direct Proof. For any integer x, ($\dagger$) says that $3x + 5$ and $5x + 2$, in summing to an odd number, have *opposite parity.* ∎

The last argument in fact proves that $3x + 5$ is even *if and only if* $5x + 2$ is odd: the converse of our claim comes for free! Look back at ($*$): you should believe that all the arrows are reversible.

[12] While what follows is a theorem, we'll typically reserve the word for results that are worth remembering in their own right. Examples like this are good for practice (change the numbers!), but are not individually very interesting.

Such variety is one of the things that makes proving theorems fun! While your choice of proof is largely a matter of personal taste, remember your audience. The final argument is very slick but might risk confusing a reader rather than empowering them.[13]

Three Proofs of the Same Result We finish this section with three proofs of the same result. All are based on the same factorization of a polynomial

$$x^3 + 2x^2 - 3x - 10 = (x-2)(x^2 + 4x + 5) = (x-2)\left[(x+2)^2 + 1\right]$$

and the well-known fact that $ab = 0 \iff a = 0$ or $b = 0$ (see Exercise 14). Since the mathematics is so simple, pay attention to and compare the *logical structures.*

Example 2.31. Let x be a real number. Then $x^3 + 2x^2 - 3x - 10 = 0 \implies x = 2$.

Direct Proof. Suppose $x^3 + 2x^2 - 3x - 10 = 0$. By factorization, $(x-2)[(x+2)^2 + 1] = 0$, so at least one of the factors must be zero. Since $(x+2)^2 + 1 \geq 1 > 0$, we conclude that $x - 2 = 0$, from which $x = 2$. ∎

Contrapositive Proof. Suppose $x \neq 2$. Since $(x+2)^2 + 1 \geq 1 > 0$, we see that

$$x^3 + 2x^2 - 3x - 10 = (x-2)[(x+2)^2 + 1] \neq 0$$

∎

Contradiction Proof. Suppose $x^3 + 2x^2 - 3x - 10 = 0$ and $x \neq 2$. Then

$$0 = x^3 + 2x^2 - 3x - 10 = (x-2)[(x+2)^2 + 1]$$

Since $x \neq 2$, we have $x - 2 \neq 0$. It follows that $(x+2)^2 + 1 = 0$. However, $(x+2)^2 + 1 \geq 1$ for all real numbers x, so we have a contradiction. ∎

Exercises 2.3. A self-test quiz and several worked questions can be found online.

1. Prove or disprove the following conjectures.
   (a) There is an even integer which can be expressed as the sum of three even integers.
   (b) Every even integer can be expressed as the sum of three even integers.
   (c) There is an odd integer which can be expressed as the sum of two odd integers.
   (d) Every odd integer can be expressed as the sum of three odd integers.
2. For any given integers a, b, c, if a is even and b is odd, prove that $7a - ab + 12c + b^2 + 4$ is odd.
3. Prove that if n is an integer greater than 1, then $n! + 2$ is even.
   ($n! = n(n-1)(n-2)\cdots 1$ *is the* factorial *of the integer* n)
4. (a) Let $x \in \mathbb{Z}$. Prove that $5x + 3$ is even if and only if $7x - 2$ is odd.
   (b) Can you conclude anything about $7x - 2$ if $5x + 3$ is odd?

[13] The Hungarian mathematician Paul Erdős referred to simple, elegant proofs as 'from the Book,' as if the Almighty kept a tome of perfect proofs. As with all matters spiritual, one person's Book might be very different to another's...

5. Consider the following proposition, where x is assumed to be a real number.

$$x^3 - 3x^2 - 2x + 6 = 0 \implies x = 3$$

   (a) Is the proposition true or false? Justify your answer. Is its converse true?
   (b) Repeat part (a) for the proposition $x^3 - 3x^2 - 2x + 6 = 0 \implies x \neq 3$.

6. Below is the proof of a result. What result is being proved?

Proof. Assume that x is odd. Then $x = 2k + 1$ for some integer k. Then

$$2x^2 - 3x - 4 = 2(2k+1)^2 - 3(2k+1) - 4 = 8k^2 + 2k - 5 = 2(4k^2 + k - 3) + 1$$

Since $4k^2 + k - 3$ is an integer, $2x^2 - 3x - 4$ is odd. ■

7. Here is another proof. What is the result this time?

Proof. Assume, without loss of generality, that $x = 2a$ and $y = 2b$ are both even. Then

$$xy + xz + yz = (2a)(2b) + (2a)z + (2b)z = 2(2ab + az + bz)$$

Since $2ab + az + bz$ is an integer, $xy + xz + yz$ is even. ■

8. Consider the following proof of the fact that (for m an integer) if m^2 is even, then m is even. Can you re-write the proof so that it doesn't use contradiction?

Proof. Suppose that m^2 is even and m is odd. Write $m = 2k + 1$ for some integer k. Then

$$m^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

is odd. Contradiction. ■

9. Here is a 'proof' that every real number x equals zero. Find the mistake.

$$\begin{aligned} x = y &\implies x^2 = xy \implies x^2 - y^2 = xy - y^2 \\ &\implies (x-y)(x+y) = (x-y)y \\ &\implies x + y = y \\ &\implies x = 0 \end{aligned}$$

10. Prove or disprove: An integer n is even if and only if n^3 is even.

11. Let n and m be positive integers. Prove n^2m is even if and only if n and m are not both odd.

12. Let x and y be integers. Prove $x^2 + y^2$ is even **if and only if** x and y have the same parity.

13. Let n be an integer. Prove $n^2 + n + 58$ is even.

14. Suppose $a, b \in \mathbb{R}$. Prove that $ab = 0 \iff a = 0$ or $b = 0$.

15. Numbers of the form $\frac{k(k+1)}{2}$, where k is a positive integer, are called *triangular numbers*. Prove that n is the square of an odd number if and only if $\frac{n-1}{8}$ is triangular.

2.4 Further Proofs & Strategies

The arguments in this section are slightly trickier and more representative of typical mathematical proofs. Some of these results are famous and worth knowing in their own right. We will also introduce *lemmas* and *corollaries*, which are used to break up the presentation of complex results.

Proving Universal Statements

Most of the results we've seen thus far have been universal statements. As discussed on page 14, any theorem $P(x) \implies Q(x)$ is implicitly universal, albeit with the quantifier $\forall x$ being typically hidden. Revisit Examples 2.24 on multiple quantifiers so see how these fit into our proof framework; here is another example.

Example 2.32. $\forall x \geq 0, \exists y < 0$ such that $x^3 < y^2$

View the claim as an implication "$x \geq 0 \implies (\exists y < 0$ such that $x^3 < y^2)$" and prove directly.

> *Proof.* Suppose $x \geq 0$ is given. *Define* $y = -\sqrt{x^3} - 1$, then $y \leq -1 < 0$ and
>
> $$y^2 = x^3 + 1 + 2\sqrt{x^3} \geq x^3 + 1 > x^3$$
>
> ∎

Notice how y, in being existentially quantified *after* x, is allowed to depend on x. We'll revisit this shortly to see what happens when we reverse the quantifiers. Remember that you might need some scratch work to find a suitable y: you shouldn't (yet!) expect to create such an argument in one shot.

For a more involved example of a universal result, here is a famous inequality relating the arithmetic and geometric means of two numbers.

Theorem 2.33 (AM–GM inequality). *If x, y are non-negative real numbers, then*

$$\frac{x+y}{2} \geq \sqrt{xy}$$

with equality if and only if $x = y$.

If your faith is wavering, first try an example: e.g., $\frac{3+5}{2} = 4 \geq \sqrt{15}$. It should also be clear that both sides are equal whenever $y = x$. The logical structure $\forall x, y \geq 0, Q(x, y)$ can be viewed as an implication $P(x, y) \implies Q(x, y)$, where $P(x, y)$ is "$x, y \geq 0$." The real challenge is making sense of $Q(x, y)$. There are really two separate results here:

1. If $x, y \geq 0$, then $\frac{x+y}{2} \geq \sqrt{xy}$
2. If $x, y \geq 0$, then $\frac{x+y}{2} = \sqrt{xy} \iff x = y$

Concentrate on the first since it is simpler. The hypothesis ($x, y \geq 0$) doesn't give us much to work with, so it seems sensible to play with the inequality and try to get rid of the ugly square-root:

$$\frac{x+y}{2} \geq \sqrt{xy} \implies (x+y)^2 \geq 4xy \implies x^2 - 2xy + y^2 \geq 0 \implies (x-y)^2 \geq 0$$

Now we have something we believe! The question is whether we can reverse the arrows. Only the first should give you any pause: it is here that we use the non-negativity of x, y.

Proof. Suppose $x, y \geq 0$. Multiply out a trivial inequality:

$$\begin{aligned}(x-y)^2 \geq 0 \iff x^2 - 2xy + y^2 \geq 0 &\iff x^2 + 2xy + y^2 \geq 4xy \\ &\iff (x+y)^2 \geq 4xy \\ &\iff \frac{x+y}{2} \geq \sqrt{xy}\end{aligned}$$

The square-root is well-defined because $x, y \geq 0$, and the inequality is preserved since the square-root function is *increasing*. For the second result, observe that the final inequality is an *equality* precisely when *all* the inequalities are equalities; this is if and only if $x = y$. ∎

The scratch work really helped us figure out how and where to apply the hypothesis. Notice also how the second result came almost for free! Result 1 only need the ($\Rightarrow$) in the proof, but the second result needs them all to be biconditional.

For variety, here is a contradiction proof incorporating the same calculations in a different order.

Contradiction Proof. Let $x, y \geq 0$ and suppose that $\frac{x+y}{2} < \sqrt{xy}$. Since $x + y \geq 0$, the second inequality holds if and only if $(x+y)^2 < 4xy$. Now multiply out and rearrange:

$$\begin{aligned}(x+y)^2 < 4xy &\iff x^2 + 2xy + y^2 < 4xy \\ &\iff x^2 - 2xy + y^2 < 0 \\ &\iff (x-y)^2 < 0\end{aligned}$$

Contradiction (squares of real numbers are non-negative). We conclude that $\frac{x+y}{2} \geq \sqrt{xy}$.
Now suppose that $\frac{x+y}{2} = \sqrt{xy}$. Following the biconditionals in the above argument, we see that equality holds if and only if $(x-y)^2 = 0$, from which we recover $x = y$. ∎

The AM–GM inequality in fact holds for any finite collection of non-negative numbers $x_1, \ldots, x_n$:

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \cdots x_n}$$

with equality if and only if all the x_i are equal. Proving this is a lot harder (see Exercise 15).

Disproving Existential Statements: Non-existence Proofs

Of the four possible combinations "prove/disprove a universal/existential statement," we've now tackled three; what remains is to consider how to prove that something does not, or cannot, exist. Recall our basic rule of negation:

$$\neg\big(\exists x, Q(x)\big) \iff \forall x, \neg Q(x)$$

To show that $\exists x, Q(x)$ is *false* is therefore to prove a *universal* statement.[14] As before (page 14), let $P(x)$ be the proposition "x lies in the domain of Q." We conclude that

$$\boxed{\neg\big(\exists x, Q(x)\big) \text{ is logically equivalent to } P(x) \implies \neg Q(x)}$$

[14]The notation $\nexists x, Q(x)$ is discouraged because it obscures this essential fact.

Once viewed as an implication, any of our proof strategies might be applicable. Contradiction and contrapositive arguments are particularly common however, since the right hand side is already a *negative* statement.

Example 2.34. The equation $x^{17} + 12x^3 + 13x + 3 = 0$ has no positive (real number) solutions.

Before seeing a proof, consider several ways in which this claim could be presented.

Non-existence $(\neg(\exists x, Q(x)))$	There are no $x > 0$ for which $x^{17} + 12x^3 + 13x + 3 = 0$.
Universal $(\forall x, \neg Q(x))$	For all $x > 0$, we have $x^{17} + 12x^3 + 13x + 3 \neq 0$.
Direct $(P \Rightarrow \neg Q)$	If $x > 0$, then $x^{17} + 12x^3 + 13x + 3 \neq 0$.
Contrapositive $(Q \Rightarrow \neg P)$	If $x^{17} + 12x^3 + 13x + 3 = 0$, then $x \leq 0$.
Contradiction $(P \wedge Q)$	$x > 0$ and $x^{17} + 12x^3 + 13x + 3 = 0$ is *impossible.*

We present two very similar arguments based on the direct and contradiction structures.

Direct proof. Suppose that $x > 0$. But then $x^{17} + 12x^3 + 13x + 3 > 0$ since all terms are positive. We conclude that $x^{17} + 12x^3 + 13x + 3 \neq 0$. ■

Contradiction proof. Assume that $x > 0$ satisfies $x^{17} + 12x^3 + 13x + 3 = 0$. Since all terms on the left hand side are positive, we have a contradiction. ■

In practice, some version of one of these arguments would likely be given without any additional commentary. The reader is assumed to be familiar with the underlying logic without it being spelled out. Our discussion could be considered scratch work.

Subdividing Theorems: Lemmas & Corollaries

Sometimes it is useful to break a proof into pieces, akin to viewing a computer program as a collection of subroutines that you combine for some greater purpose. Often the intention is to improve the readability of a difficult/complex argument, but you may also wish to (de-)emphasize the relative importance of certain results. Mathematics does this by using *lemmas* and *corollaries.*

Lemma: A theorem whose importance you want to downplay or which will be used when proving a more significant result.

Corollary: A theorem which follows quickly once you understand another result, perhaps as a special case or by modifying the proof in some small way.

Presentation style varies hugely between authors and journals: some reserve *theorem* only for the most important results, with everything else presented as a lemma or corollary, while others never use these terms (or just call everything a *proposition*!). Regardless, lemmas and corollaries are useful to have in your toolkit if readability is your goal.

In preparation for our next, much more important, result, here is a simple lemma.

Lemma 2.35. *Suppose n is an integer. Then n^2 is even $\iff$ n is even.*

At this stage, you should be able to prove this yourself. This is really just a special case of Theorem 2.29: if you're completely unsure how to start, revisit that result, and the rest of Section 2.3.

Irrational Numbers

Since their definition is inherently negative, irrational numbers provide good examples of non-existence/contradiction arguments. They are also interesting in their own right!

Definition 2.36. A real number x is *rational* if it may be written in the form $x = \frac{m}{n}$ for some integers m, n. A real number is *irrational* if no such integers exist.

You likely know of a few irrational numbers ($\sqrt{2}, \pi, e$), but how do we *prove* that a given number is irrational? Our next result is very famous, with versions dating back at least to Aristotle (c. 340 BCE).

Theorem 2.37. *$\sqrt{2}$ is irrational.*

We must *disprove* the existence claim $\exists m, n \in \mathbb{Z}, \sqrt{2} = \frac{m}{n}$. As before, consider several restatements:

Non-existence	There are no integers m, n for which $\sqrt{2} = \frac{m}{n}$.
Universal	For all integers m, n, we have $\sqrt{2} \neq \frac{m}{n}$.
Direct	If $m, n \in \mathbb{Z}$, then $\sqrt{2} \neq \frac{m}{n}$.
Contrapositive	If $\sqrt{2} = \frac{m}{n}$, then m, n are not both integers.
Contradiction	$m, n \in \mathbb{Z}$ and $\sqrt{2} = \frac{m}{n}$ is *impossible.*

Can you see the obvious drawbacks of the direct and contrapositive versions? We instead present a proof by contradiction. We outsource a repeated argument to Lemma 2.35 to improve readability.

Proof. Suppose that $m, n \in \mathbb{Z}$ and that $\sqrt{2} = \frac{m}{n}$. *Without loss of generality*, assume that m, n have no common factors. Cross-multiply and square:

$$m^2 = 2n^2 \text{ is even } \implies m \text{ is even} \qquad \text{(Lemma 2.35)}$$

whence $m = 2k$ for some integer k. But then

$$2n^2 = m^2 = 4k^2 \implies n^2 = 2k^2 \text{ is even } \implies n \text{ is even} \qquad \text{(Lemma 2.35)}$$

We see that m and n have a common factor of 2. Contradiction. ∎

The major difficulty lies in the assumption that m, n have no common factors. In the same way that we can simplify $\frac{4}{6} = \frac{2}{3}$, our assumption is *without loss of generality* because it costs us nothing *once we assume $\sqrt{2} = \frac{m}{n}$ is rational.* It is crucial to appreciate that we aren't contradicting the assumption that m, n have no common factors, lest our calculation continue forever without resolution!

$$m^2 = 2n^2 \implies n^2 = 2k^2 \implies k^2 = 2l^2 \implies \cdots$$

The irrationality of $\sqrt{3}, \sqrt[3]{2}$, etc., can be proved similarly (π and e are *much* harder!). Now we have the theorem, it is easily applied to demonstrate the irrationality of many other numbers.

Example 2.38. Suppose that $\sqrt{2} - 5\sqrt{3} = x$ were rational: $\exists m, n \in \mathbb{Z}$ such that $x = \frac{m}{n}$. Then

$$75 = (5\sqrt{3})^2 = (\sqrt{2} - x)^2 = 2 + x^2 - 2\sqrt{2}x \implies \sqrt{2} = \frac{x^2 - 73}{2x} = \frac{m^2 - 73n^2}{2mn}$$

Otherwise said, $\sqrt{2}$ is *rational*: contradiction.

Non-constructive Existence Proofs

Every existence proof we've seen so far has been *constructive*: we exhibit/construct an *explicit example* x for which $Q(x)$ is true. Sometimes, however, this is expecting a bit too much. It is often far easier to show the existence of something *without* explicitly stating what it is. We present two famous examples of this situation.

Theorem 2.39. *There are irrational numbers a, b for which a^b is rational.*

Proof. Consider the number $x = (\sqrt{2})^{\sqrt{2}}$. There are two possibilities:

1. x is rational. Let $a = b = \sqrt{2}$.
2. x is irrational. Let $a = x$ and $b = \sqrt{2}$ and apply the usual exponential laws to see that

$$a^b = \left((\sqrt{2})^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\cdot\sqrt{2}} = (\sqrt{2})^2 = 2$$

In either case, a, b are irrational and a^b rational. ∎

The proof is very sneaky: it does not provide an explicit example and does not tell us whether $(\sqrt{2})^{\sqrt{2}}$ is rational. In fact this number isn't rational, though demonstrating it is massively harder.[15]

We finish with a particularly famous example of a non-constructive existence proof found in Euclid's *Elements* (300 BCE), the most influential textbook of mathematical history. As ever, we need a solid definition before we try to prove anything.

Definition 2.40. An integer ≥ 2 is *prime* if the only positive integers it is divisible by are itself and 1.

The first few primes are $2, 3, 5, 7, 11, 13, 17, 19, \ldots$ It follows, though it is not completely obvious, that every integer ≥ 2 is either prime or a product of primes (*composite*). In particular, every integer ≥ 2 is divisible by at least one prime. We now state Euclid's result, and prove it by contradiction.

Theorem 2.41 (*Elements*, Book IX, Prop. 20). *There are infinitely many prime numbers.*

Proof. Assume there are exactly n primes $p_1, \ldots, p_n$ and define the integer

$$\Pi := p_1 \cdots p_n + 1$$

Certainly Π is divisible by some prime p_i (in our list by assumption!), as is the product $p_1 \cdots p_n$. But then the difference

$$1 = \Pi - p_1 \cdots p_n$$

is divisible by p_i, contradicting the fact that $p_i \geq 2$. ∎

[15] If you're interested, look up the Gelfond–Schneider Theorem (1934), Hilbert's Seventh Problem, and what they say about *algebraic* and *transcendental numbers.* Such ideas are far beyond the level of this text!

Exercises 2.4. A self-test quiz and worked questions can be found online.

1. Prove or disprove: There exists a line L in the plane such that, for all points A, B in the plane, we have that A, B lie on L.

2. Prove or disprove:

   (a) There exist integers m and n such that $2m - 3n = 15$.

   (b) There exist integers m and n such that $6m - 3n = 11$.

3. Prove: For every positive integer n, the integer $n^2 + n + 3$ is odd and greater than or equal to 5.

4. Let p be an odd integer. Prove that the equation $x^2 - x - p = 0$ has no *integer* solutions.

5. Prove or disprove the following conjectures about real numbers x, y.

   (a) If $3x + 5y$ is irrational, then at least one of x and y is irrational.

   (b) If x and y are rational, then $3x + 4xy + 2y$ is rational.

   (c) If x and y are irrational, then $3x + 4xy + 2y$ is irrational.

6. Prove by contradiction: if x and y are positive real numbers, then $\sqrt{x+y} \neq \sqrt{x} + \sqrt{y}$.

7. Prove that between any two distinct rational numbers there exists another rational number.

8. Consider the proposition:

   For any non-zero rational number r and any irrational number t, the number rt is irrational.

   (a) Translate this statement into logic using quantifiers and propositional functions.

   (b) Prove the statement.

9. (a) Prove that an integer n^2 is divisible by 3 if and only if n is divisible by 3. Hence prove that $\sqrt{3}$ is irrational.

   (b) Prove that $\sqrt[3]{2}$ is irrational. (*Hint: revisit Exercise 2.3.10*)

10. Here is an alternative argument that $\sqrt{2}$ is irrational using the *method of infinite descent*, which is very important in number theory.

    Suppose that $\sqrt{2} = \frac{m}{n}$ where m, n are positive integers; this time we don't assume that m, n have no common factors.

    (a) Prove that there exist positive integers m_1, n_1 which satisfy three conditions:

    $$m_1^2 = 2n_1^2, \qquad m_1 < m, \qquad n_1 < n$$

    (b) Argue that there exist two sequences of decreasing positive integers $m > m_1 > m_2 > \cdots$ and $n > n_1 > n_2 > \cdots$ which satisfy $m_i^2 = 2n_i^2$ for each i.

    (c) Is it possible to have an infinite sequence of decreasing *positive* integers? Why not? Hence complete the argument that $\sqrt{2}$ is irrational.

11. We extend Example 2.34 as you might have seen it in calculus. Use the following facts to give a formal proof that $x^{17} + 12x^3 + 13x + 3 = 0$ has *exactly one solution* x, and that x lies in the interval $(-1, 0)$.

   - All polynomials are continuous.
   - (Intermediate Value Theorem) If f is continuous on the interval $[a, b]$ and L lies between $f(a)$ and $f(b)$, then $f(x) = L$ for some $x \in (a, b)$.
   - If $f'(x) > 0$ on an interval, then f is an increasing function.

12. Euclid's original argument for Theorem 2.41 is slightly different. He asserts the following:

   > Given a list of primes $p_1, \ldots, p_n$, the number $\Pi := p_1 \cdots p_n + 1$ is divisible by a *new prime* not in the list.

   Rewrite the proof following Euclid's approach.

13. The real numbers satisfy the *Archimedean property*:

   > For any $x, y > 0$, there exists a positive integer n such that $nx > y$.

   (a) Use the Archimedean property to show that there are no positive real numbers which are less than $\frac{1}{n}$ for all positive integers n.

   (b) Consider the following 'proof' of the fact that every real number is less than some positive integer:

   > *Proof.* Consider a real number x. For example, $x = 19.7$. Then $x < 20$ and 20 is a positive integer. ■

   What is wrong with this argument? Give a correct proof.

   (c) Prove: $\forall x, y \in \mathbb{R}$ with $x < y$, $\exists m, n \in \mathbb{Z}$ for which $nx < m < ny$. Hence conclude an extension of Exercise 7: between any two *real* numbers there exists a rational number.

   (d) (Hard) Is it true that between any two real numbers there exists an *irrational* number? If so, prove it.

14. Use the AM–GM inequality (two-variable or full version) to answer the following.

   (a) Suppose $x, y, z \geq 0$ satisfy $x + y + z = 1$.

      i. What is the largest possible value of xyz?

      ii. (Hard) Prove that $(1 - x)(1 - y)(1 - z) \geq 8xyz$.

   (b) Prove: $n! \leq \left(\frac{n+1}{2}\right)^n$. (*Hint: find a formula for the sum of the first n positive integers*)

15. We prove the full AM–GM inequality.

   (a) When $n = 3$, try mimicking our earlier approach by cubing the desired inequality. Why does this seem unwise?

   (b) (Hard) Prove that $x \leq e^{x-1}$ for all real numbers x, with equality if and only if $x = 1$. (*Hint: Use calculus! Consider $f(x) = e^{x-1} - x$ and apply a derivative test or Maclaurin series*)

   (c) Let $\mu = \frac{x_1 + x_2 + \cdots + x_n}{n}$ be the arithmetic mean. Apply part (b) to each expression $x = \frac{x_i}{\mu}$ to conclude that $x_1 \cdots x_n \leq \mu^n$ and hence complete the proof.