2 An introduction to proofs

Before we talk about proofs, we give a very brief guide to the basics of a mathematical theory.

2.1 The basics of a mathematical theory

We begin with a collection of

- **Axioms**: propositions that we agree in advance are true.

Axioms may be thought of as the fundamental building blocks of any mathematical theory. They are usually chosen to be simple, intuitive statements that capture the essential structure of the objects that we want in our theory. You may be a little dissatisfied by a supposedly "rigorous" mathematical course starting out by making unprovable "assumptions"; but remember, we can do *nothing* unless we have *something* to build from!

A famous example of a set of axioms is the set of five that Euclid used in his book *Elements* to lay down the ground rules of the mathematical system that we now call "Euclidean geometry"[15][16][17]:

1. A straight line segment can be drawn joining any two points.
2. Any straight line segment can be extended indefinitely in a straight line.
3. Given any straight line segment, a circle can be drawn having the segment as radius and one endpoint as center.
4. All right angles are congruent.
5. If two lines are drawn which intersect a third in such a way that the sum of the inner angles on one side is less than two right angles, then the two lines inevitably must intersect each other on that side if extended far enough. (This axiom is equivalent to what is known as the "parallel postulate": parallel lines don't meet.)

[15] Statements taken from http://mathworld.wolfram.com/EuclidsPostulates.html.

[16] Why not just "Geometry"? For over two millennia after Euclid proposed his five axioms, mathematicians struggled with the fifth of them. The first four were obvious, simple, necessary building blocks of geometry, but the fifth seemed overly complex. Generations of mathematicians attempted to reduce the complexity of the axioms by *proving* (in the sense that we are using in this section) the fifth axiom from the first four. All attempts were unsuccessful, and in 1823, Janos Bolyai and Nicolai Lobachevsky independently discovered why: there are systems of geometry that satisfy the first four axioms of Euclid, but not the fifth; that is, there are entirely consistent notions of geometry in which sometimes parallel lines *do* eventually meet. So to describe geometry in the plane, as Euclid was trying to do, something like the complex fifth axiom is needed. Systems of geometry that satisfy the first four axioms of Euclid, but not the fifth, are referred to as "non-Euclidean geometries".

[17] These are actually Euclid's five *postulates*; his *axioms* define the basic properties of equality. We will mention these later.

(As another example of a set of axioms, consider the fundamental building blocks of the United States laid down by the founding fathers in the Declaration of Independence:

> "We hold these truths to be self-evident, that all men are created equal, that they are endowed by their creator with certain unalienable rights, that among these are life, liberty and the pursuit of happiness.")

Along with axioms, we have

- **Definitions**: statements that specify what particular terms mean.

Think of the list of definitions as a dictionary, and the list of axioms as a rule-book. As an example, Euclid presents four definitions, explaining what words like "point" and "line" (used in the axioms) mean[18][19]:

1. A *point* is that which has no part.
2. A *line* is a breadthless length.
3. The extremities of lines are points.
4. A straight line lies equally with respect to the points on itself.

Once we have Axioms and Definitions, we move on to the meat of a mathematical theory, the

- **Theorems**: statements whose truth follows from the axioms and the definitions via rules of logical inference.

If the definitions are the dictionary, and the axioms are the rule-book, then the theorems are the structures that can be legitimately formed from the words, "legitimately" meaning following the rules of the rule-book. As an example, here is Euclid's famous Theorem I.47, the *Pythagorean theorem*[20]:

> **Theorem**: In right-angled triangles the square on the side opposite the right angle equals the sum of the squares on the sides containing the right angle.

How do we know that the Pythagorean theorem is indeed a theorem, that is, is indeed a statement that follows Euclid's rule-book? We know, because Euclid provided a *proof* of the theorem, and once we follow that proof we have no choice but to accept that if we agree with the axioms, we must agree with the Pythagorean theorem.

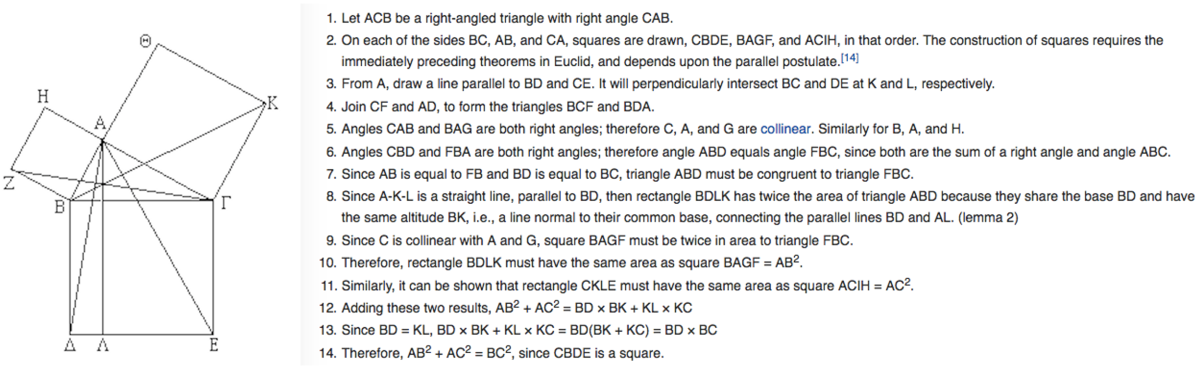
[18] Statements taken from http://www-history.mcs.st-and.ac.uk/HistTopics/Euclid_definitions.html.

[19] As pointed out at http://www-history.mcs.st-and.ac.uk/HistTopics/Euclid_definitions.html, these seem a little strange, as Euclid seems to be defining "point" twice (first and third definitions), and "line" twice (second and fourth). Fortunately we don't need to worry about this, as Math 10850 is not a course in Euclidean geometry!

[20] Statement from https://www.cut-the-knot.org/pythagoras/Proof1.shtml.

- **Proofs**: the truth of a statement p is established via a *proof*, a sequence of statements, ending with the statement p, each of which is either
  - an axiom,
  - an instance of a definition,
  - a theorem that has previously been proved, or
  - a statement that follows from some of the previous statements via a rule of inference.

For completeness, here's a treatment of Euclid's proof of the Pythagorean theorem, as presented in Wikipedia:



1. Let ACB be a right-angled triangle with right angle CAB.
2. On each of the sides BC, AB, and CA, squares are drawn, CBDE, BAGF, and ACIH, in that order. The construction of squares requires the immediately preceding theorems in Euclid, and depends upon the parallel postulate.[14]
3. From A, draw a line parallel to BD and CE. It will perpendicularly intersect BC and DE at K and L, respectively.
4. Join CF and AD, to form the triangles BCF and BDA.
5. Angles CAB and BAG are both right angles; therefore C, A, and G are collinear. Similarly for B, A, and H.
6. Angles CBD and FBA are both right angles; therefore angle ABD equals angle FBC, since both are the sum of a right angle and angle ABC.
7. Since AB is equal to FB and BD is equal to BC, triangle ABD must be congruent to triangle FBC.
8. Since A-K-L is a straight line, parallel to BD, then rectangle BDLK has twice the area of triangle ABD because they share the base BD and have the same altitude BK, i.e., a line normal to their common base, connecting the parallel lines BD and AL. (lemma 2)
9. Since C is collinear with A and G, square BAGF must be twice in area to triangle FBC.
10. Therefore, rectangle BDLK must have the same area as square BAGF = AB^2.
11. Similarly, it can be shown that rectangle CKLE must have the same area as square ACIH = AC^2.
12. Adding these two results, $AB^2 + AC^2 = BD \times BK + KL \times KC$
13. Since $BD = KL$, $BD \times BK + KL \times KC = BD(BK + KC) = BD \times BC$
14. Therefore, $AB^2 + AC^2 = BC^2$, since CBDE is a square.

A proof of the Pythagorean, by Euclid

2.2 Proofs, more slowly

In the last section we said what a proof is, slightly formally. Now we'll look much more closely at the notion of proof, starting more informally. Quoting Hutchings [2]:

> "A mathematical proof is an argument which convinces other people that something is true. Math isn't a court of law, so a 'preponderance of the evidence' or 'beyond any reasonable doubt' isn't good enough. In principle we try to prove things beyond any doubt at all."

We've discussed in the last section the grammar and vocabulary that will be used to present proofs; nor we turn to the rather more exciting and challenging process of actually production proofs. Let's begin with an example, a dialogue between Alice and Bob (two frequently occurring characters in mathematics) taken verbatim from Hutchings [2] (the footnotes are mine).

Alice I've just discovered a new mathematical truth!

Bob Oh really? What's that?

Alice For every integer x, if x is even, then x^2 is even.

Bob Hmm… are you sure that this is true?

Alice Well, isn't it obvious?

Bob No, not to me.

Alice OK, I'll tell you what. You give me any integer x, and I'll show you that the sentence 'if x is even, then x^2 is even' is true. Challenge me.

Bob (eyes narrowing to slits): All right, how about $x = 17$.

Alice That's easy. 17 is not even, so the statement 'if 17 is even, then 17^2 is even' is vacuously true[21]. Give me a harder one.

Bob OK, try $x = 62$.

Alice Since 62 is even, I guess I have to show you that 62^2 is even.

Bob That's right.

Alice (counting on her fingers furiously): According to my calculations, $62^2 = 3844$, and 3844 is clearly even…

Bob Hold on. It's not so clear to me that 3844 is even. The definition says that 3844 is even if there exists an integer y such that $3844 = 2y$. If you want to go around saying that 3844 is even, you have to produce an integer y that works.

Alice How about $y = 1922$.

Bob Yes, you have a point there. So you've shown that the sentence 'if x is even, then x^2 is even' is true when $x = 17$ and when $x = 62$. But there are billions[22] of integers that x could be. How do you know you can do this for every one?

Alice Let x be any integer.

Bob Which integer?

[21] Think about the implication "p implies q". It's the same as "(not p) or q". If p is false (as in this case: p is the statement "17 is an even number") then "not p" is true, so the disjunction "(not p) or q" is indeed true. And this is going to be the case regardless of what p and q are. This is what Alice means when she says that 'if 17 is even, then 17^2 is even' is vacuously true; and more generally, the statement 'p implies q' is vacuously true whenever p is false. This idea is so universally understood, that we (almost) never refer to it when proving implications.

On the other hand, if p is true (as will happen in a moment, when x is set to 62), then "not p" is false, so the only way we are going to show that the disjunction "(not p) or q" is true is by showing that q is true. Of course, we get to use the fact that p is true in the argument, which will probably be a big help!

[22] Billions? Actually infinitely many!

Alice Any integer at all. It doesn't matter which one. I'm going to show you, using only the fact that x is an integer and nothing else, that if x is even then x^2 is even.

Bob All right . . . go on.

Alice So suppose x is even.

Bob But what if it isn't?

Alice If x isn't even, then the statement 'if x is even, then x^2 is even' is vacuously true. The only time I have anything to worry about is when x is even.

Bob OK, so what do you do when x is even?

Alice By the definition of 'even', we know that there exists at least one integer y such that $x = 2y$.

Bob Only one, actually.

Alice I think so[23]. Anyway, let y be an integer such that $x = 2y$. Squaring both sides of this equation, we get $x^2 = 4y^2$. Now to prove that x^2 is even, I have to exhibit an integer, twice which is x^2.

Bob Doesn't $2y^2$ work?

Alice Yes, it does. So we're done.

Bob And since you haven't said anything about what x is, except that it's an integer, you know that this will work for any integer at all.

Alice Right.

Bob OK, I understand now.

Alice So here's another mathematical truth. For every integer x, if x is odd, then x^2 is. . .

Two comments are in order here (the first paraphrased from [2]):

- A proof is an explanation which convinces someone that a statement is true. A good proof also helps them understand *why* it is true.
- The proof we have just given is long (though we will soon start presenting proofs much more compactly) but, importantly, it has only *finite* length. And yet, it is verifying *infinitely many* things: 2^2 is even, 4^2 is even, 6^2 is even, 8^2 is even, and so on. This is a first illustration of the remarkable power of mathematical logic — we have, in a finite amount of space, verified infinitely many truths!

[23] But it doesn't really matter — we just need *at least one* such y.

In this course, we will prove (almost) everything that we discuss. It might make sense, then, that we start the semester off with a thorough introduction to proofs and logic. We won't, though. We will instead learn about proofs mostly by *doing* them. For the rest of this section, we'll just discuss fairly briefly some of the common techniques of proofs, with simple examples to illustrate some of them. Then we will move on to the *real* examples, and develop a familiarity with proofs by exposure and immersion.

2.3 A summary of basic proof techniques

Here, taken from [2], is a table ("Table 1: Logic in a nutshell") that summarizes, informally, "just about everything you will need to know about logic. It lists the basic ways to prove, use, and negate every type of statement. In boxes with multiple items, the first item listed is the one most commonly used. Don't worry if some of the entries in the table appear cryptic at first; they will make sense after you have seen some examples."

Statement	Ways to Prove it	Ways to Use it	How to Negate it
p	• Prove that p is true. • Assume p is false, and derive a contradiction.	• p is true. • If p is false, you have a contradiction.	not p
p and q	• Prove p, and then prove q.	• p is true. • q is true.	(not p) or (not q)
p or q	• Assume p is false, and deduce that q is true. • Assume q is false, and deduce that p is true. • Prove that p is true. • Prove that q is true.	• If $p \Rightarrow r$ and $q \Rightarrow r$ then r is true. • If p is false, then q is true. • If q is false, then p is true.	(not p) and (not q)
$p \Rightarrow q$	• Assume p is true, and deduce that q is true. • Assume q is false, and deduce that p is false.	• If p is true, then q is true. • If q is false, then p is false.	p and (not q)
$p \iff q$	• Prove $p \Rightarrow q$, and then prove $q \Rightarrow p$. • Prove p and q. • Prove (not p) and (not q).	• Statements p and q are interchangeable.	(p and (not q)) or ((not p) and q)
$(\exists x \in S)\ P(x)$	• Find an x in S for which $P(x)$ is true.	• Say "let x be an element of S such that $P(x)$ is true."	$(\forall x \in S)$ not $P(x)$
$(\forall x \in S)\ P(x)$	• Say "let x be any element of S." Prove that $P(x)$ is true.	• If $x \in S$, then $P(x)$ is true. • If $P(x)$ is false, then $x \notin S$.	$(\exists x \in S)$ not $P(x)$

Table 1: Logic in a nutshell.

Note that in the fifth row (Statement $p \iff q$), second column (Ways to Prove it), you should read "Prove p and q" to mean "prove p (is true), and, in a separate argument, prove q (is true)", rather than "prove the conjection 'p and q"', and the same for "Prove (not p) and (not q)". Also, for all statements involving quantifiers, the table takes "S" to be the universe of discourse.

2.4 Examples of proofs

Here we present a list of examples of using proof techniques. The statements we will prove will all be very simple ones. This is fine; the point of this section is not to derive deep truths, but rather to illustrate the techniques that we will be using repeatedly as the year goes on, on many rather more serious examples.

Most of the examples here are taken from [2], essentially verbatim.

An example of proving a "for every" statement

This first example involves proving a 'for every' statement, but can also be thought of as proving an implication — an 'if ... then' statement. Along the way we will see how to leverage knowing that a 'there exists' statement happens to be true. All of these ideas have been already introduced in Alice and Bob's dialogue.

Example: Give a proof that for every integer x, if x is odd, then $x + 1$ is even.

This is a 'for every' statement, so the first thing we do is write

> Let x be any integer.

Think of x as a particular integer here ... 11, or -2, or 1729, just one that we are not explicitly naming. If we can show that 'if x is odd then $x + 1$ is even', using *only* that fact that x is an integer, and not using any properties of a particular integer, then we will have shown that *for all integers* x, if x is odd, then $x + 1$ is even, as required.

Again, we have to show, using only the fact that x is an integer, that if x is odd then $x + 1$ is even. As discussed earlier, this implication is vacuously true if x happens to be even, so we get to assume from here on that x is odd. So we write

> Suppose x is odd.

We must somehow use this assumption to deduce that $x + 1$ is even. Now the statement 'x is odd' means 'there exists an integer y such that $x = 2y + 1$'. So we get to leverage the assumption 'x is odd', by writing x in the form $2y + 1$, where y is *known for certain* to be an integer[24]. So we write

> Let y be an integer such that $x = 2y + 1$ (such a y exists because x is odd).

[24] Which integer? We don't know; it depends on what x is, and we haven't said explicitly what x is. But that's ok; all we are going to use is that y is *some* integer.

Note that we don't just write "Let y be an integer such that $x = 2y + 1$" and leave it at that; we need to justify that such a y actually exists, hence the comment in parentheses.

Now we want to prove that $x + 1$ is even. In other words, we want to show that there exists an integer y such that $x + 1 = 2y$. **BUT**, we have to be careful! The name 'y' is already in use; it is a witness to the fact that x is odd. So in telling ourselves what we mean by the statement '$x + 1$ is even', we need to use a different name for the witness. That's fine, as there are lots of available names. Let's use w. We write

> To show that $x + 1$ is even, we need to find an integer w such that $x + 1 = 2w$.

How do we find such a w? Well, we know $x = 2y+1$, so $x+1 = (2y+1)+1 = 2y+2 = 2(y+1)$, so it looks like we have a candidate w, namely $y + 1$. We finish the proof by writing

> Adding 1 to both sides of $x = 2y + 1$, we get
>
> $$x + 1 = (2y + 1) + 1, \quad \text{or, equivalently,} \quad x + 1 = 2(y + 1).$$
>
> Since y is an integer, so is $y + 1$. Taking $w = y + 1$ we see that $x + 1$ is even.

Notice that we haven't just explained how $x + 1$ gets written in the forn $2w$ — we have also justified that the w in question *is an integer*, which is part of the definition of $x + 1$ being even.

The proof is now done. It's typical to insert a symbol to indicate that a proof has come to an end. Historically that symbol was often the string "Q.E.D." (*quod erat demonstrandum*, Latin for "what was to be shown"[25]). It is much more common these days to use the symbol "□".

Here's how the proof would look without the extraneous discussion:

Claim: For every integer x, if x is odd, then $x + 1$ is even.

Proof: Let x be any integer. Suppose x is odd. Let y be an integer such that $x = 2y + 1$ (such a y exists because x is odd). To show that $x + 1$ is even, we need to find an integer w such that $x + 1 = 2w$. Adding 1 to both sides of $x = 2y + 1$, we get

$$x + 1 = (2y + 1) + 1, \quad \text{or, equivalently,} \quad x + 1 = 2(y + 1).$$

Since y is an integer, so is $y + 1$. Taking $w = y + 1$ we see that $x + 1$ is even. □

Notice that

- the proof is written in *prose*. When read out loud (reading the symbols in the usual way we say them; "equals" for "=", et cetera) it makes perfect sense as a paragraph in ordinary language, and

[25] Or: "quite easily done".

- every step of the proof is justified: every line follows from previous ones, by an application of a definition, or by an appeal to something which has been established as true earlier in the prrof.

These two properties are hallmarks of a good proof, and you should strive towards them in your proof writing!

An example of a proof involving an "and" statement

Example: Write a proof that for every integer x and[26] for every integer y, if x is odd and y is odd then xy is odd.

As before we begin

> Let x and y both be integers. Suppose x and y are both odd.

Because we are assuming that *both* x *and* y are odd, we can leverage *both* of these statements to provide alternate ways of representing *both* x *and* y. And since the fact that both x and y are odd is the *only* thing that we know about these two numbers, using the definition of oddness to represent them in terms of other integers is basically the *only* thing that we can do to have any hope of proceeding with this particular proof. So we write

> Then there are integers w and v such that $x = 2w + 1$ and $y = 2v + 1$.

Two things are worth noting here. The first is that to prove the result in its full generality, we have to use different names for the witnesses that x and y are odd. It would not do to say that there is integer w such that $x = 2w + 1$ and integer w such that $y = 2w + 1$. If we did this, we would be implicitly forcing x and y to be equal for the rest of the proof, and would end up proving the much more restrictive statement that if x, y are both odd, and equal, then xy is odd — in other words, if x is odd so is x^2.

The second point worth noting is that we are already engaging in a very common practice in the writing of mathematical proofs, that of skipping steps that are obvious enough not to be spelled out. In this case, what we really should have written is something like:

> Since x is odd and y is odd, it follows that in particular x is odd. So there exists an integer w such that $x = 2w + 1$.
>
> Also, since x is odd and y is odd, it follows that in particular y is odd. So there exists an integer v such that $y = 2v + 1$.

[26] This 'and' is not a logical 'and'; it is just there to make the statement easier to read. Some people might write "for all integers x, y" here. Symbolically, what we are being asked to prove involves a double universal qualifier, and can be written

$$(\forall x \in \mathbb{Z})(\forall x \in \mathbb{Z})(((x \text{ odd}) \wedge (y \text{ odd})) \Rightarrow (xy \text{ odd})).$$

That is, we should have inferred "p" from "p and q", and drawn our first conclusion; and then inferred "q" from "p and q", and drawn our second conclusion. But this really is overkill![27]

We want to conclude that xy is odd, and there is really only one thing we can do: use the two expressions we have derived for x and y to derive a new expression for xy, and see if we can "massage" it into the form "twice an integer, plus one". That's easily done, so we go straight to the formal write-up:

> We now have
>
> $$xy = (2w+1)(2v+1) = 4wv + 2w + 2v + 1 = 2(2wv + w + v) + 1.$$
>
> Since v and w are integers, so is $2wv + w + v$, so we conclude that xy is odd. □

Here's the full proof in one pass:

> Let x and y both be integers. Suppose x and y are both odd. Then there are integers w and v such that $x = 2w + 1$ and $y = 2v + 1$.
>
> We now have
>
> $$xy = (2w+1)(2v+1) = 4wv + 2w + 2v + 1 = 2(2wv + w + v) + 1.$$
>
> Since v and w are integers, so is $2wv + w + v$, so we conclude that xy is odd. □

An example of an "if and only if" proof

Remember that "p if and only if q", sometimes abbreviated to "p iff q", is shorthand for the conjunction

$$(p \text{ implies } q) \text{ and } (q \text{ implies } p).$$

As such, proofs of if-and-only-if statements usually require two distinct parts:

- a proof that p implies q,

and

- a proof that q implies p.

In the example we are about to give, the two parts are quite similar, but in general they might use quite different techniques.

Claim: For every integer x, x is even if and only if $x + 1$ is odd.

Proof: We begin by proving that for every integer x, if x is even then $x + 1$ is odd. Indeed, let x be any even integer. There is an integer y such that $x = 2y$, so $x + 1 = 2y + 1$, showing that $x + 1$ is odd.

[27] Knowing what steps to skip, because they are obvious enough not to be spelled out, is a witchy art, not a science, and depends a lot on your own mathematical maturity, and your understanding of the mathematical maturity of your audience. It is an art that we will feel our way into as the year goes on.

Next we prove that for every integer x, if $x+1$ is odd then x is even. Indeed, let x be any integer such that $x+1$ is odd. There is an integer y such that $x+1=2y+1$, so $x=2y$, showing that x is even. □

Notice that the proof was written quite compactly, with some of the justifications elided. For example, we didn't say that it is from the definition of evenness that "x is even" allows us to conclude "there is an integer y with $x=2y$". This is an example of me understanding my audience — we have seen a number of proofs now involving evenness and oddness, so I don't feel the need any more to spell out that I am using the definition. Nonetheless, the proof is still written *using full sentences*, with *no substantial step left unjustified*.

The value of this if-and-only-if proof is that now we can conclude that for any integer x, the statements 'x is even' and '$x+1$ is odd' are interchangeable; this means that we can take any true statement and replace some occurrences of the phrase 'x is even' with the phrase '$x+1$ is odd' to get another true statement; and, more importantly, we can do this *without having to provide a proof to justify the exchange* — once the equivalence has been proven once, it remains true for all time, and can be used as part of our arsenal of basic true statements. For example, in their dialogue Alice and Bob proved that

> For every integer x, if x is even then x^2 is even.

Since "x is even" is now known to be interchangeable with "$x+1$ is odd", we can conclude, without need for further proof, that the following is also a true statement:

> For every integer x, if $x+1$ is odd then x^2 is even.

Proof by cases

Sometimes it is very helpful to break a proof into cases, with the different possible cases being treated differently (sometimes slightly differently, sometimes substantially so). Let's start with an example (from which the general method should be very apparent), before discussion the matter more formally.

Example: Prove that for every integer x, the number $x(x+1)$ is even.

Some integers are even, some are odd, none are both, and every integer is one of the two.[28] So it makes a great deal of sense to consider first what happens when x is even, and then what happens when x is odd. If we can establish that

- if x is even, then $x(x+1)$ is even

[28] This is obvious, no? Formally, it requires a proof: x being even means that there is an integer y with $x=2y$, while x being odd means that there is an integer y' with $x=2y'+1$. It's not unreasonable that there might be some number z that can be expressed both as $2y$ and $2y'+1$, for some integers y,y'; and/or that there might be some number z that *cannot* be expressed as either $2y$ or $2y'+1$, for any integers y,y'. Of course, neither such z exists, but it actually takes some effort to prove. We'll defer it until we have seen prove by induction.

and

- if x is odd, then $x(x+1)$ is even

then we will have covered all possibilities, and shown that no matter what sort of integer x is, $x(x+1)$ is even.

The details of the proof are quite easy, so what follows is mainly introduced as a template for the presentation of proofs by cases.

Proof: We consider two cases.

Case 1, x even In this case there is an integer y such that $x = 2y$. We have $x + 1 = 2y + 1$, so

$$x(x+1) = (2y)(2y+1) = 4y^2 + 2y = 2(2y^2 + y).$$

Since $2y^2 + y$ is an integer, this shows that in this case $x(x+1)$ is even.

Case 2, x odd In this case there is an integer y such that $x = 2y+1$. We have $x+1 = 2y+2$, so

$$x(x+1) = (2y+1)(2y+2) = 4y^2 + 6y + 2 = 2(2y^2 + 3y + 1).$$

Since $2y^2 + 3y + 1$ is an integer, this shows that in this case $x(x+1)$ is even.

The two cases cover all possibilities, so we conclude that $x(x+1)$ is always even. □

Formally, here's what's going on in a proof by cases: we are trying to prove the implication "P implies q", and we realize that the predicate P can be expressed as "p_1 or p_2 or $\cdots$ or p_n", for some simpler predicates $p_1, \ldots, p_n$. So really what we are trying to prove is that

$$(p_1 \text{ or } p_2 \text{ or } \cdots \text{ or } p_n) \text{ implies } q. \tag{1}$$

(In the example just given, P is "x is an integer", p_1 is "x is an even integer" and p_2 is "x is an odd integer"). Instead of proving this single implication, we proceed by cases, proving each of the implications "p_1 implies q", "p_2 implies q", et cetera. From this we immediately conclude that the following statement is true:

$$(p_1 \text{ implies } q) \text{ and } (p_2 \text{ implies } q) \text{ and } \cdots \text{ and } (p_n \text{ implies } q). \tag{2}$$

Is this enough to conclude (1)? It's left as an exercise for the reader[29] to argue that in fact (1) and (2) are equivalent.

Proofs by cases are often quite tedious![30]. For example:

Claim: If $1 \leq n \leq 40$ then $n^2 - n + 41$ is a prime number.

Proof: The hypothesis here is the disjunction (the "or") of 40 separate cases: $n = 1$, $n = 2$, et cetera. So to complete the proof, it's enough to check each of those cases in turn:

[29] This is often code for: the author is too lazy to write down the details. But in these notes, "exercise for the reader" will usually be code for: look out for this on a homework/quiz/exam.

[30] I've seen plenty of research papers where at one point the authors have to deal with Case 7, Subcase C, Subsubcase viii, or some such!

- Case 1 ($n = 1$): Here $n^2 - n + 41 = 41$, which is indeed a prime number.
- Case 2 ($n = 2$): Here $n^2 - n + 41 = 43$, which is again a prime number.
- Case 3 ($n = 3$): Here $n^2 - n + 41 = 47$, again a prime number.
- Cases 4 through 39 ($n = 4$ through 39): Left to reader[31]
- Case 40 ($n = 40$): Here $n^2 - n + 41 = 1601$, which is a prime number[32].

□

Indirect proofs (contradiction and contrapositive)

All of the proof examples we have presented so far have been what are usually called *direct* proofs: we verified various implications of the form "p implies q" by assuming that p is true, and then *directly* arguing, via definitions, rules of logic, and earlier established truths, that q inevitably must be true.

Sometimes it is easier to argue indirectly. The most common form of an indirect argument is *proof by contradiction*: suppose that we want to prove that the statement p is true. We begin by assuming that p is false. We then try to deduce a contradiction, that is, some statement q which we know is false. If we succeed, then our assumption that p is false must be wrong! So p must be true, and our proof is finished.

To be a little more specific: often, when arguing that an implication "p implies q" is true, we begin by assuming that p is true and q is false (the one situation in which the implication "p implies q" is false) and derive a contradiction, meaning: we deduce that some statement r is true, and also that its negation "not r" is true, so that "r and (not r)" is true. This can't be (the truth value of "r and (not r)" is always false). So the only possible conclusion is that it is *not* the case that p is true and q is false, which is the same as saying that it *is* the case that "p implies q" is true.

Example (Here the universe of discourse for all variables is the set of real numbers): Prove the statement "If $5x + 25y = 2019$, then at least one of x, y is not an integer".

Proof: We argue by contradiction. Let us assume both that $5x + 25y = 2019$ and that both of x, y are integers (this is the negation of "at least one of x, y is not an integer"). We have that

$$5x + 25y = 5(x + 5y),$$

so $5x + 25y$ is a multiple of 5; and since $5x + 25y = 2019$, this says that 2019 is a multiple of 5. But also, by a direct calculation, we see that 2019 is *not* a multiple of 5. We have arrived at a contradiction, and so conclude that the statement we are trying to prove is indeed true. □

Some comments are in order:

[31] Here really because of the author's laziness.

[32] How do I know? I asked https://www.isprimenumber.com/prime/1601.

- Why didn't we try a direct proof? Because assuming the truth of the hypothesis in this case (that $5x + 25y = 2019$) gives us very little to work with — it tells us nothing specifically about x and y.

- In this example of proof by contradiction, we had p:"$5x + 25y = 2019$", q:"at least one of x, y is not an integer", and r:"2019 is a multiple of 5".

Another indirect proof technique is *proof by contrapositive*: this involves proving "p implies q" by giving a *direct* proof of the statement "(not q) implies (not p)". This is the contrapositive of, and equivalent to, "p implies q). By "giving a direct proof" I mean assuming "not q" and then using axioms, definitions, logical equivalences and rules of inference to deduce "not p".

Example: Prove "if mn is even, then either m is even or n is even".

Proof: We give a direct proof of the contrapositive statement: if both m and n are odd, then mn is odd.

Let us assume that m and n are odd. Then there are whole numbers k and ℓ with $m = 2k + 1$ and $n = 2\ell + 1$. We have

$$\begin{aligned} mn &= (2k+1)(2\ell+1) \\ &= 2k\ell + 2k + 2\ell + 1 \\ &= 2(k\ell + k + \ell) + 1. \end{aligned}$$

Since $k\ell + k + \ell$ is a whole number, mn is odd. □

A few comments are in order on this example:

- Proof by contrapositive can be thought of as a special case of proof by contradiction: we assume p and "not q", and reach the contradiction "p and (not p).

- Why didn't we try a direct proof here? Because, as in the last example, assuming the truth of the hypothesis in this case (that mn is even) gives us very little to work with — it tells us nothing specifically about m and n.

- Most of the serious proofs that we will see in this course will either be proofs by contradiction, or proofs by contrapositive.

Various other examples of proving implications

Most of the theorems we will prove will have statements of the form "if X holds then Y holds", where X is a string of assumptions, which we will call the *hypotheses* of the theorem, and Y is the *conclusion*. This is an implication: "X implies Y". So in discussing proofs, we will mostly be concerned with ways of rigorously justifying implications.

Suppose we are faced with the implication "p implies q", and we want to prove that it is valid. Here are two more proof techniques we can use. Both of them are slightly degenerate, but important to know about.

- **Trivial proof**: If we know q is true then $p \Rightarrow q$ is true regardless of the truth value of p.

  Example: (For this example, and most subsequent examples in this section, the universe of discourse for all variables is the set of positive natural numbers. The exceptions to this convention will be noted as we come across them). "If n is a prime number, then $n - n = 0$". Here the conclusion "$n - n = 0$" is true, whether n is a prime number or not; so the implication is *trivially* true.

- **Vacuous proof**: If we know p is false then "p implies q" is true regardless of the truth value of q (we've discussed this earlier, in a footnote during Alice and Bob's dialogue).

  Example 1: "If $4n$ is a prime number, then $n - n = 0$". Here the hypothesis is "$4n$ is a prime number". But this is *false*, regardless of what n we pick ($4n$ will always be a multiple of 4). So, by the truth table of implication, the implication is *true*, and we can say this without even looking at the conclusion statement.

  Here's another way to look at this, which explains why we refer to this as a "vacuous" proof: to prove the implication, we are being asked to verify that *whenever it holds that* $4n$ *is prime, it also holds that* $n - n = 0$. It *never* holds that $4n$ is prime, so there are *no* cases to check, there is no possible witnesses to the *incorrectness* of the implication, so, having no evidence to the contrary, we must conclude that the implication is *correct*.

  Example 2: "If $4n$ is a prime number, then $n - n = 1$". In Example 1 we could have equally well argued that the implication is trivial(ly true), since the conclusion is true. Here, the conclusion is *false*. But again, the *implication* is true, vacuously. The premise is false, and so there are no witnesses to refute the implication.

  These examples should illustrate that implication is a subtle (you might say "slippery") logical operation, that takes some getting used to.

2.5 An note on equality

We haven't said it explicitly yet, but it has been implicit: in proving statements involving numbers, as well as using the rules of inference, axioms, definitions, and logical equivalences, we also use a few basic properties of the equality symbol "=", namely:

- **E1**: For all numbers a, $a = a$ ("Things which coincide with one another are equal to one another.")

- **E2**: For all a, b and c, if $a = c$ and $b = c$ then $a = b$ ("Things which are equal to the same thing are also equal to one another.")

- **E3**: For all a, b, c and d, if $a = b$ and $c = d$ then $a + c = b + d$ and $a - c = b - d$ ("If equals are added to equals, the whole are equal" and "If equals be subtracted from equals, the remainders are equal.")

These "axioms of equality" were first formulated by Euclid around 300BC; I've put his statements in parentheses above[33].

2.6 A (slightly) more formal look at logic

For those who might be interested, we say a little bit more here about the formal business of logic and proofs. In reality we won't need to use any of this language as the year progresses, so reading this section is *entirely* optional, and I won't mention any of this in class or quizzes.

Rules of inference

The rules of inference are the basic rules of logic, that allow us to infer, or deduce, the truth of new propositions from old. Each rule is a re-statement of a tautology. Take "Hypothetical syllogism" below as an example. Suppose I know that

> If Notre Dame beats Michigan this year, I will celebrate with beer at Rohr's

(this is an axiom: how else would I celebrate?) and also that

> If I drink beer at Rohr's, I will Uber home

(again an axiom: I don't drink and drive). Then I should legitimately be able to conclude

> If Notre Dame beats Michigan this year, I will Uber home that night.

Why can I conclude this? Because the statement

$$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$$

is a *tautology*; it's a true statement, regardless of the truth values that p, q and r happen to take. (In this case p:"Notre Dame beats Michigan", q:"I celebrate" and r:"I Uber home".)

Once we've verified that the relevant propositions are tautologies, each of the rules of inference should be quite palatable. Here is the list of rules that we will most commonly use:

Name	If you know ...	you can infer ...	because ... is a tautology
Modus ponens	p and $p \Rightarrow q$	q	$(p \wedge (p \Rightarrow q)) \Rightarrow q$
Modus tollens	$\neg q$ and $p \Rightarrow q$	$\neg p$	$(\neg q \wedge (p \Rightarrow q)) \Rightarrow \neg p$
Disjunction introduction	p	$p \vee q$	$p \Rightarrow (p \vee q)$
Conjunction elimination	$p \wedge q$	p	$(p \wedge q) \Rightarrow p$
Hypothetical syllogism	$p \Rightarrow q$ and $q \Rightarrow r$	$p \Rightarrow r$	$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
Conjunction introduction	p and q	$p \wedge q$	$(p \wedge q) \Rightarrow (p \wedge q)$
Disjunctive syllogism	$p \vee q$ and $\neg p$	q	$((p \vee q) \wedge (\neg p)) \Rightarrow q$
Constructive dilemma	$p \Rightarrow q, r \Rightarrow s$ and $p \vee r$	$q \vee s$	$((p \Rightarrow q) \wedge (r \Rightarrow s) \wedge (p \vee r))$ $\Rightarrow q \vee s$

[33] Wording taken from http://www.friesian.com/space.htm.

In the next few paragraphs, we'll make some remarks on the rules of inference. This section won't have many examples, because soon we will launch into the main topic of the first half of the course, working with the axioms of the real numbers, and we will get a chance there to see plenty of proofs that use these methods.

- **Modus ponens**: If you know p, and you know p implies q, you can deduce q.

  The name comes from the Latin phrase *modus ponendo ponens*, meaning *the way that affirms by affirming*, conveying the sense that modus ponens is quite a direct method of inference. It is by far the most used and most important method.

- **Modus tollens**: If you know that p implies q, and you know that q is *false*, you can deduce that p is false.

  The name comes from the Latin phrase *modus tollendo tollens*, meaning *the way that denies by denying*, conveying the sense that modus tollens is an *indirect* method of inference. It is sometimes called *proof by contrapositive*, because the contrapositive of "p implies q" is (the equivalent statement) "not q implies not p", and knowing this together with "not q" allows the immediate deduction of "not p", by modus ponens.

  The next few rules are quite obvious and require no discussion:

- **Disjunction introduction**: If you know that p is true, then regardless of the truth or otherwise of some other statement q, you can immediately deduce that at least one of p or q are true.

- **Conjunction elimination**: If you know that both p and q are true, then you can immediately deduce that p is true.

- **Hypothetical syllogism**: If you know that p implies q, and that q implies r, then (by following the obvious chain) you can deduce that p implies r. This says that "implies" is a *transitive* relation.

- **Conjunction introduction**: If you know that both p and q are true, then you can deduce that the compound statement "p and q" is true. This is a sort of converse to Conjunction elimination.

- **Disjunctive syllogism**: If you know that either p or q are true, and you know that p is false, then you can deduce that q is true.

- **Constructive dilemma**: If you know both that p implies q, and that r implies s, and you also know that at least one of the two premises p, r are true, then (since you can deduce that at least one of the conclusions q, s are true), you can deduce that the compound statement "r or s" is true.

This is a “constructive dilemma” because you deduce that one of two things (q or s) is true, but you have no way of knowing explicitly *which* is true; you can’t “construct” a simple true statement out of the knowledge that the complex statement “q or s” is true.

An note on *invalid* inferences

Modus ponens says: from p and $p \Rightarrow q$ you can infer q, and modus tollens says: from $\neg q$ and $p \Rightarrow q$ you can infer $\neg p$.

There are two other tempting “rules of inference” that are both **INVALID**:

- “from q and $p \Rightarrow q$ you can infer p”: this is called *affirming the consequent*, or the *converse error* (using the *conclusion* to say something about the *hypothesis*), and is invalid, because

$$(q \wedge (p \Rightarrow q)) \Rightarrow p$$

  is not a tautology.
- “from $p \Rightarrow q$ you can infer $(\neg p) \Rightarrow (\neg q)$”: this is called *denying the antecedent*, or the *inverse error* (confusing the direction of implication), and is invalid, because

$$(p \Rightarrow q) \Rightarrow ((\neg p) \Rightarrow (\neg q))$$

  is not a tautology.

Let’s illustrate all of this with the statement:

> “If you fall of a wall, you break a bone”.

This is an implication, with hypothesis “you fall off a wall” and conclusion “you break a bone”.

- Suppose you know that the implication is true, and you also know that you fell off a wall. Then you conclude that you broke a bone. That is modus ponens in action.
- Suppose you know that the implication is true, and you also know that you *do not* have a broken bone. Then you conclude that you *did not* fall off a wall. That is modus tollens in action.
- Suppose you know that the implication is true, and you also know that you have a broken bone. Then you *cannot* conclude that you fell off a wall — there are other ways to break a bone. If you did make that inference, you would be making the converse error.

- Suppose you know that the implication is true. Then you *cannot* conclude that if you do not fall off a wall, then you do not have a broken — again, this implication is easily shown to be false by considering any non-falling-off-a-wall circumstance that leads to a broken bone. If you did make that inference, you would be making the inverse error.

There are also some rules of inference relating to quantification, all of which are quite evident:

- **Universal instantiation**: If you know $(\forall x)p(x)$, you can infer $p(c)$ for any particular c in the universe of discourse
- **Universal generalization**: If you know $p(c)$ for an arbitrary/generic element in the universe of discourse, you can infer $(\forall x)p(x)$
- **Existential instantiation**: If you know $(\exists x)p(x)$, you can infer $p(c)$ for some c in the universe of discourse (this allows you to define a variable c to stand for some fixed element of the universe of discourse, whose specific name may not be known, for which $p(c)$ is true)
- **Existential generalization**: If you know $p(c)$ for some fixed element of the universe of discourse you can infer $(\exists x)p(x)$.

Approaches to proving quantified statements

Often the statements of theorems are of the form $(\exists x)p(x)$ or $(\forall x)p(x)$. Here we discuss some general approaches to these types of theorems.

- **Constructive existential proofs**: To prove $(\exists x)p(x)$, one approach is to find ("construct") an explicit element c in the universe of discourse for x, such that $p(c)$ is true.

  Example: "There exist arithmetic progressions of length 4, all terms of which are prime numbers".

  Proof: The numbers 251, 257, 263 and 269 form an arithmetic progressions of length 4, and all of these numbers are prime.

- **Non-constructive existential proofs**: One can sometimes prove $(\exists x)p(x)$ by showing that there must be an element c in the universe of discourse for x, such that $p(c)$ is true, *without explicitly exhibiting such a c.*

  Example: "Among any 13 people, some two of them must have their birthdays in the same month".

Proof: Let k_i be the number of people, among the 13, who have their birthday in the ith month of the year. We want to show $k_i \geq 2$ for some i. Suppose, for a contradiction, that $k_i \leq 1$ for each i. Then

$$k_1 + k_2 + \cdots + k_{12} \leq 1 + 1 + \cdots + 1 = 12.$$

But since everybody has a birth-month, we also have

$$k_1 + k_2 + \cdots + k_{12} = 13$$

That $k_1 + \cdots + k_{12}$ is simultaneously at most 12 and exactly 13 is a contradiction, and this proves the statement.

Some remarks:

- The principle exposed in this proof is sometimes called the *pigeon-hole principle*: "If more than n pigeons distribute themselves among at most n pigeon holes, then there must be at least one pigeon-hole that has at least two pigeons in it". This simple-sounding principle turns out to be incredibly powerful ('though unfortunately quite hard to apply!) Some applications appear in the homework.
- There are quite a few major open problems in the field of combinatorics (a brach of mathematics closely related to theoretical computer science) that involve finding *constructive* existential proofs of statements that are very easy proven in a non-constructive way.

- **Non-existence proofs**: Suppose we wish to show that there is *no* element of the universe of discourse that satisfies a particular predicate; that is, we wish to prove $\neg(\exists x)p(x)$. This is equivalent to $(\forall x)(\neg p(x))$; so one approach is to choose a generic element c in the universe of discourse for x, assume that $p(c)$ holds, and derive a contradiction. This allows us to conclude that for generic c, $\neg p(c)$ is true, and so (by universal generalization) $(\forall x)(\neg p(x))$ is true.

  Example: (Here the universe of discourse for m is positive whole numbers). "There is no m for which $4m + 3$ is a perfect square".

  Proof: Let m be an arbitrary positive integer, and assume that $4m + 3$ is a perfect square, say $4m + 3 = k^2$ for some integer k. Because $4m + 3$ is odd, so too is k^2; and because the square of an even number is even, it must be that k is an odd number, say $k = 2a + 1$ for some integer a. So we have

$$4m + 3 = (2a + 1)^2.$$

  Rearranging terms, this is equivalent to

$$2 = 4(a^2 + a - m),$$

and this implies, dividing both sides by 2, that

$$1 = 2(a^2 + a - m).$$

This is a contradiction: the left-hand side above is odd, and the right-hand side is even (since $a^2 + a - m$ is a whole number). This contradiction shows that $4m + 3$ is never a perfect square.

- **Universal quantification proofs**: In general to establish $(\forall x)p(x)$ one starts with a generic element c of the universe of discourse, and argues the truth of $p(c)$. We will see plenty of examples going forward.

- **Counterexamples**: Sometimes we want to establish $\neg(\forall x)p(x)$ — that is is *not* the case that $p(c)$ is true for every element of the universe of discourse. What is required here is an example of a *single*, *specific* c in the universe of discourse for which $p(c)$ is *false*. This is often referred to as a *counterexample* to the statement $(\forall x)p(x)$.

  Example (actually, exercise): We've seen that $n^2 - n + 41$ is prime for $1 \leq n \leq 40$. Show that is *not* true that $n^2 - n + 41$ is prime for every positive integer n.