What is a Proof?

A ***proof*** is a method of establishing truth. This is done in many different ways in everyday life:

Jury trial. Truth is ascertained by twelve people selected at random.

Word of God. Truth is ascertained by communication with God, perhaps via a third party.

Experimental science. The truth is guessed and the hypothesis is confirmed or refuted by experiments.

Sampling. The truth is obtained by statistical analysis of many bits of evidence. For example, public opinion is obtained by polling only a representative sample.

Inner conviction. "*My* program is perfect. I know this to be true."

"I don't see why not..." Claim something is true and then shift the burden of proof to anyone who disagrees with you.

Intimidation. Truth is asserted by someone with whom disagreement seems unwise.

Mathematics its own notion of "proof". In mathematics, a ***proof*** is a verification of a ***proposition*** by a chain of ***logical deductions*** from a base set of ***axioms***. Each of the three highlighted terms in this definition is discussed in a section below. The last section contains some complete examples of proofs.

1 Propositions

A *proposition* is a statement that is either true or false. This definition sounds very general and is a little vague, but it does exclude sentences such as, "What's a surjection, again?" and "Learn logarithms!" Here are some examples of propositions.

Proposition 1. $2 + 3 = 5$

This proposition happens to be true.

If you suspect you've found an error in these notes or you just find a part hopelessly confusing, please send email to e_lehman@mit.edu, and I'll try to fix the problem.

Proposition 2. $\forall\, n \in \mathbb{N} \quad n^2 + n + 41$ *is a prime number.*

This proposition is more complicated. The symbol $\forall$ is read "for all", and the symbol $\mathbb{N}$ stands for the set of natural numbers, $\{0, 1, 2, 3, \ldots\}$. (There is some disagreement about whether 0 is a natural number; in this course, it is.) So this proposition asserts that the final phrase is true for all natural numbers n. That phrase is actually a proposition in its own right:

$$\text{"}n^2 + n + 41 \text{ is a prime number"}$$

In fact, this is a special kind of proposition called a ***predicate***, which is a proposition whose truth depends on the value of one or more variables. This predicate is certainly true for *many* natural numbers n:

$\mathbf{n}$	$\mathbf{n^2 + n + 41}$	**prime or composite?**
0	41	prime
1	43	prime
2	47	prime
3	53	prime
...	...	(all prime)
20	461	prime
39	1601	prime

Experimental data like this can be useful in mathematics, but can also be misleading. In this case, when $n = 40$, we get $n^2 + n + 41 = 40^2 + 40 + 41 = 41 \cdot 41$, which is not prime. So Proposition 2 is actually false!

Proposition 3. $a^4 + b^4 + c^4 = d^4$ *has no solution when* $a, b, c, d \in \mathbb{N}^+$.

Here $\mathbb{N}^+$ denotes the *positive* natural numbers, $\{1, 2, 3, \ldots\}$. In 1769, Euler conjectured that this proposition was true. But then it was proven false 218 years later by Noam Elkies at the liberal arts school up Mass Ave. He found the solution $a = 95800, b = 217519, c = 414560, d = 422481$. We could write his assertion symbolically as follows:

$$\exists\, a, b, c, d \in \mathbb{N}^+ \quad a^4 + b^4 + c^4 = d^4$$

The $\exists$ symbol is read "there exists". So, in words, the expression above says that there exist positive natural numbers a, b, c, and d such that $a^4 + b^4 + c^4 = d^4$.

Proposition 4. $313(x^3 + y^3) = z^3$ *has no solution when* $x, y, z \in \mathbb{N}^+$.

This proposition is also false, but the smallest counterexample has more than 1000 digits. This counterexample could never have been found by a brute-force computer search!

The symbols $\forall$ ("for all") and $\exists$ ("there exists") are called ***quantifiers***. A quantifier is always followed by a variable (and perhaps an indication of what values that variable can take on) and then a predicate that typically involves that variable. The predicate may itself involve more quantifiers. Here are a couple examples of statements involving quantifiers:

$$\exists\, x \in \mathbb{R} \quad x^2 - x + 1 = 0$$
$$\forall\, y \in \mathbb{R}^+ \quad \exists\, z \in \mathbb{R} \quad e^z = y$$

The first statement asserts that the equation $x^2 - x + 1 = 0$ has a real solution, which is false. The second statement says that as z ranges over the real numbers, e^z takes on every positive, real value at least once.

Proposition 5. *In every map, the regions can be colored with 4 colors so that adjacent regions have different colors.*

This proposition was conjectured by Guthrie in 1853. The proposition was "proved" in 1879 by Kempe. His argument relied on pictures and— as is often the case with picture-proofs— contained a subtle error, which Heawood found 11 years later. In 1977, Appel and Haken announced a proof that relied on a computer to check an enormous number of cases. However, many mathematicians remained unsatisfied because no human could hand-check the computer's work and also because of doubts about other parts of the argument. In 1996, Robertson, Sanders, Seymour, and Thomas produced a rigorous proof that still relied on computers. Purported proofs of the Four Color Theorem continue to stream in. For example, I. Cahit unveiled his 12-page solution in August 2004, but here is his proof of Lemma 4: "Details of this lemma is left to the reader (see Fig. 7)." Don't try that on your homework! Even if this one doesn't hold up, some day a simple argument may be found.

Proposition 6. *Every even integer greater than 2 is the sum of two primes.*

For example, $24 = 11 + 13$ and $26 = 13 + 13$. This is called the Goldbach Conjecture, after Christian Goldbach who first stated the proposition in 1742. Even today, no one knows whether the conjecture is true or false. Every integer ever checked is a sum of two primes, but just one exception would disprove the proposition.

Proposition 7. $\forall\, n \in \mathbb{Z} \quad (n \geq 2) \Rightarrow (n^2 \geq 4)$

The symbol $\mathbb{Z}$ denotes the set of integers, $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$. There is predicate nested inside this proposition:

$$(n \geq 2) \Rightarrow (n^2 \geq 4)$$

This is an example of an ***implication***, a proposition of the form $P \Rightarrow Q$. This expression is read "P implies Q" or "if P, then Q". The proposition correctly asserts that this particular

implication is true for every integer n. In general, *the implication $P \Rightarrow Q$ is true when P is false or Q is true.* Another way of saying how implication works is with a ***truth table***:

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

In general, a truth table indicates whether a compound proposition is true or false for every possible truth setting of the constituent propositions. The second line of this table, for example, says that the implication $P \Rightarrow Q$ is false when P is true and Q is false.

Just now we used variables (P and Q) to denote arbitrary propositions. We'll often use such ***Boolean variables*** in place of specific propositions. These are variables that can take on only two possible values, true or false, just as the propositions they represent could be either true or false.

Here another example of an implication:

"If pigs fly, then you will understand the Chernoff Bound."

This is no insult! It's a true proposition, even if you're planning to sleep like a baby through the entire Chernoff Bound lecture. The reason is that the first part of the implication ("pigs fly") is false. And the last two lines of the truth table say that *$P \Rightarrow Q$ is always true when P is false.* This might not be the way you interpret if-then statements in everyday speech, but it's the accepted convention in mathematical discussions.

Proposition 8. $\forall\, n \in \mathbb{Z} \quad (n \geq 2) \Leftrightarrow (n^2 \geq 4)$

A proposition of the form $P \Leftrightarrow Q$ is read "P if and only if Q". (Sometimes "if and only if" is abbreviated "iff".) This proposition is true provided *P and Q are both true or both false*. Put another way, $P \Leftrightarrow Q$ is true provided *$P \Rightarrow Q$ and $Q \Rightarrow P$ are both true.* Here is a truth table that compares all these kinds of implication:

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

The predicate $(n \geq 2) \Leftrightarrow (n^2 \geq 4)$ is true when $n = 1$ (because both sides are false) and true when $n = 3$ (because both sides are true) but false when $n = -3$ (because the left side is false, but the right side is true). Therefore, Proposition 8 as a whole is false.

2 Axioms

An ***axiom*** is a proposition that is assumed to be true, because you believe it is somehow reasonable. Here are some examples:

Axiom 1. *If $a = b$ and $b = c$, then $a = c$.*

This seems very reasonable! But, of course, there is room for disagreement about what constitutes a reasonable axiom. For example, one of Euclid's axioms for geometry is equivalent to the following:

Axiom 2 (Parallel Postulate). *Given a line l and a point p not on l, there is exactly one line through p parallel to l.*

In the 1800's several mathematicians realized that the Parallel Postulate could be replaced with a couple alternatives. This axiom leads to "spherical geometry":

Axiom 3. *Given a line l and a point p not on l, there is* no *line through p parallel to l.*

And this axiom generates "hyperbolic geometry".

Axiom 4. *Given a line l and a point p not on l, there are* infinitely many *lines through p parallel to l.*

Arguably, no one of these axioms is really better than the other two. Of course, a different choice of axioms makes different propositions true. And axioms should not be chosen carelessly. In particular, there are two basic properties that one wants in a set of axioms: they should be consistent and complete.

A set of axioms is ***consistent*** if no proposition can be proved both true and false. This is an absolute must. One would not want to spend years proving a proposition true only to have it proved false the next day! Proofs would become meaningless if axioms were inconsistent.

A set of axioms is ***complete*** if every proposition can be proved or disproved. Completeness is very desirable; we would like to believe that any proposition could be proved or disproved with sufficient work and insight.

Surprisingly, making a complete, consistent set of axioms is not easy. Bertrand Russell and Alfred Whitehead tried during their entire careers to find such axioms for basic arithmetic and failed. Then Kurt Gödel proved that *no* finite set of axioms for arithmetic can be both consistent and complete! This means that any set of consistent axioms is necessarily incomplete; there will be true statements that can not be proved. For example, it might be that Goldbach's conjecture is true, but there is no proof!

In this class, we will not dwell too much on the precise set of axioms underpinning our proofs. Generally, we'll regard familiar facts from high school as axioms. You may

find this imprecision regarding the axioms troublesome at times. For example, in the midst of a proof, you may find yourself wondering, "Must I prove this little fact or can I assume it?" Unfortunately, there is no absolute answer. Just be upfront about what you're assuming, and don't try to evade homework and exam problems by declaring everything an axiom!

3 Logical Deductions

Logical deductions or *inference rules* are used to combine axioms and true propositions in order to form more true propositions.

One fundamental inference rule is ***modus ponens***. This rule says that if P is true and $P \Rightarrow Q$ is true, then Q is also true. Inference rules are sometimes written in a funny notation. For example, modus ponens is written:

$$\frac{P \qquad P \Rightarrow Q}{Q}$$

This says that if you know that the statements above the line are true, then you can infer that the statement below the line is also true.

Modus ponens is closely related to the proposition $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$. Both in some sense say, "if P and $P \Rightarrow Q$ are true, then Q is true". This proposition is an example of a ***tautology***, because it is true for every setting of P and Q. The difference is that this tautology is a *single proposition*, whereas modus ponens is an inference rule that allows us to *deduce new propositions from old ones*. However, if we accept modus ponens, then a general theorem of logic says that for each tautological implication there is an associated inference rule. For example, $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$ and $((P \Rightarrow Q) \wedge \neg Q) \Rightarrow \neg P$ are both tautologies, as one can verify with truth tables, and here are the analogous inference rules:

$$\frac{P \Rightarrow Q \qquad Q \Rightarrow R}{P \Rightarrow R} \qquad\qquad \frac{P \Rightarrow Q \qquad \neg Q}{\neg P}$$

As with axioms, we won't say exactly what inference rules are legal in this class. Each step in a proof should be clear and "logical"; in particular, you should make clear what previously proved facts are used to derive each new conclusion.

4 Examples of Proofs

Let's put these ideas together and make some complete proofs.

4.1 A Tautology

Theorem 9. *The following proposition is a tautology:*

$$(X \Rightarrow Y) \quad \Leftrightarrow \quad (\neg Y \Rightarrow \neg X)$$

The expression on the right is called the ***contrapositive*** of $X \Rightarrow Y$. This theorem is asserting that an implication is true if and only if its contrapositive is true. As an everyday example, the implication:

"If you are wise, then you attend recitation."

is logically equivalent to its contrapositive:

"If you do not attend recitation, then you are not wise."

The simplest way to prove a statement involving a small number of Boolean variables, like Theorem 9, is to check all possible cases. In particular, we need to verify that the proposition is true for every setting of the Boolean variables X and Y. A truth table can help you organize such a proof and work systematically through all the cases.

Proof. We show that the left side is logically equivalent to the right side for every setting of the variables X and Y.

X	Y	$X \Rightarrow Y$	$\neg Y \Rightarrow \neg X$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Thus, the proposition $(X \Rightarrow Y) \Leftrightarrow (\neg Y \Rightarrow \neg X)$ is true in every case, which implies that it is a tautology. □

The since the tautological implication in Theorem 9 runs both ways, there are two corresponding inference rules (although they amount to about the same thing):

$$\frac{P \Rightarrow Q}{\neg Q \Rightarrow \neg P} \qquad\qquad \frac{\neg Q \Rightarrow \neg P}{P \Rightarrow Q}$$

These rules are quite useful. Sometimes when you set out to prove an implication $P \Rightarrow Q$, proving the contrapositive $\neg Q \Rightarrow \neg P$ turns out to be a bit easier or clearer. If you prove the contrapositive, then the original implication immediately follows by the second inference rule shown above.

4.2 A Proof by Contradiction

The three preceding theorems were established by ***direct proofs***; that is, we combined axioms and previously-proved theorems in a straightforward way until we reached the desired conclusion. Sometimes an ***indirect proof*** (also known as a ***proof by contradiction***) is easier. The idea is to assume that the desired conclusion is *false* and then show that that assumption leads to an absurdity or contradiction. This means that the assumption must be wrong, and so the desired conclusion is actually true.

In logical terms, indirect proof relies on the following inference rule:

$$\frac{\neg P \Rightarrow \text{false}}{P}$$

In words, if $\neg P$ implies some falsehood, then P must actually be true. We can verify this inference rule by checking that the corresponding implication is a tautology:

P	$(\neg P \Rightarrow \text{false}) \Rightarrow P$
T	T
F	T

Sure enough. Now let's see how indirect proof works in practice.

Theorem 10. *$\sqrt{2}$ is an irrational number.*

This theorem was first proved by the Pythagoreans, a secretive society dating back to about 500 BC that intertwined mysticism and mathematics. The irrationality of $\sqrt{2}$ and the existence of a twelve-sided regular polyhedron (the dodecahedron) were among their prized secrets.

Proof. In order to obtain a contradiction, assume that $\sqrt{2}$ is rational. Then we can write $\sqrt{2} = a/b$ where a and b are integers, b is nonzero, and the fraction is in lowest terms. Squaring both sides gives $2 = a^2/b^2$ and so $2b^2 = a^2$. This implies that a is even; that is, a is a multiple of 2. As a result, a^2 is a multiple of 4. Because of the equality $2b^2 = a^2$, $2b^2$ must also be a multiple of 4. This implies that b^2 is even and so b must be even. But since a and b are both even, the fraction a/b is not in lowest terms. This is a contradiction, and so the assumption that $\sqrt{2}$ is rational must be false. □

When you use indirect proof, state this clearly and specify what assumption you are making in order to obtain a contradiction. Also, remember that the intermediate statements in an indirect proof may very well be false, because they derive from a false assumption. A common mistake is to forget this and later regard these statements as true!