3.1 Direct Proofs

Some terminology.

A *definition* is an agreement on the meaning of a term.

A *proof* is a convincing mathematical argument.

Theorem	are proven statements	major statement
Proposition		minor statement
Lemma		helper statement, technical
Corollary		easily follows from another statement

Example.

To consider	you first have to know
real numbers	rational numbers
rational numbers	integers
integers	natural numbers

Eventually you come to a concept that cannot be defined in terms of another concept, or we would be going in circles. Such concepts are called *undefined terms*. Also, some properties of those concepts are not proven, but accepted. Those properties are called *axioms*. (You have to start somewhere!)

Example. When studying properties of natural numbers:

undefined terms: natural numbers, addition, $<$, 1

axiom: for every natural number n, $n + 1 > n$

Example. When studying properties of real numbers (likened to points on a line):

undefined terms: real numbers, addition, multiplication, $<$, 0, 1

some axioms: $a + (b + c) = (a + b) + c$
$a \cdot (b + c) = a \cdot b + a \cdot c$
if $a < b$, then $a + c < b + c$
if $a < b$ and $c \geq 0$, then $ac < bc$
every set that is bounded above has a least upper bound

Direct proofs of conditional statements are ones where we start with the hypothesis, make a series of logical arguments and end up at the conclusion.

Statements about divisibility of numbers are simple — we will use them to illustrate various proof methods.

Definition. A nonzero integer m *divides* an integer n if there exists an integer q such that $n = m \cdot q$. We write $m \mid n$ and say: m *divides* n, m *is a divisor of* n, or n *is a multiple of* m. Note that 0 does not divide any integer.

Theorem. Let a, b, c be integers and $a, b \neq 0$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof.

Theorem. Let a, b, c be integers and $a \neq 0$. If $a \mid b$ and $a \mid c$, then $a \mid b + c$.

Proof.

Definition. Let $n \in \mathbf{N}$, $a, b \in \mathbf{Z}$. We say a *is congruent to* b *modulo* n if n divides $a - b$. We write $a \equiv b \pmod{n}$.

Example. What is congruent to:

$5 \pmod 4$

$-3 \pmod 7$

Example. It is 14:00 hrs. What time is it in 33 hours?

Theorem. Let $a, b, c \in \mathbf{Z}$, $n \in \mathbf{N}$.
1) *(reflexivity)* For every $a \in \mathbf{Z}$, $a \equiv a \pmod{n}$.
2) *(symmetry)* If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
3) *(transitivity)* If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proof.

Proving inequalities.

Example. Show that for every $x \in \mathbf{R}$, if $x > 0$, then $x + \dfrac{1}{x} \geq 2$.

As part of investigating how to prove inequalities, it is OK to start with the conclusion and arrive at the hypothesis, but you need to check that you can retrace your steps — starting with the hypothesis, ending with the conclusion — and write the finished proof in this way.

The following example shows that there are examples where steps cannot be retraced, even though one can start with the conclusion and end with the hypothesis.

Example. "Show" that for every $x \in \mathbf{R}$, if $x \leq 1$, then $x - 3 \geq x + 1$

3.2 More Methods of Proof

Direct proofs of $P \implies Q$ went like this: start with P and logically deduce Q. Sometimes this is not convenient.

Example. Let p and q be rational numbers, $q \neq 0$. Prove: if x is irrational, then $p + qx$ is irrational.

Recall: x is irrational if it cannot be written as $\frac{a}{b}$ for some integers a, b, $b \neq 0$. So we are trying to prove:

$$x \text{ is not of form } \frac{a}{b} \implies p + qx \text{ is not of form } \frac{c}{d}$$

But the assumption of not being of a certain form doesn't give you much to work with. For example, you cannot write an equation, and expressions with $\neq$ are difficult to work with. We can try to prove the equivalent contrapositive (recall that $P \implies Q \equiv \neg Q \implies \neg P$):

$$p + qx \text{ is rational } \implies x \text{ is rational}$$

Proof.

Example. For each integer n, if n^2 is even, then n is even.

Proof.

Biconditional Statements have form P if and only if Q ($P \iff Q$). We prove them by proving two statements: 1) if P, then Q ($P \implies Q$)
2) if Q, then P ($Q \implies P$)

Example. A circle of radius r centered at point (h, k) has equation $(x-h)^2+(y-k)^2 = r^2$.

This really means: A point with coordinates (x, y) is on a circle of radius r centered at point (h, k) if and only if $(x-h)^2+(y-k)^2 = r^2$.

Proof. $\implies$*)*

$\impliedby$)

Often, the proof of $Q \implies P$ is simply the proof of $P \implies Q$ read backwards.

Proof by Construction. Often, statements of form $(\exists x)(P(x))$ can be proven by finding the x that satisfies $P(x)$.

Example. There exists a real number x such that $2x^2 - 5x - 7 = 0$.

Proof.

Example. For every positive real number x there exists
a) a number y such that $y > x$
b) a number y such that $0 < y < x$.

Proof.

Nonconstructive Proof.

Example. For an $a \in \mathbf{R}$, $a \geq 0$, we have written $\sqrt{a}$ to denote a number whose square is a. Thanks to experience with the calculator, it is plausible that such a number exists. Suppose we do not take this as a given.

Proposition. There exists a real number x such that $x^2 = 2$.

Proof. – by drawing

Proof. – by using the Intermediate Value Theorem

Theorem (IVT). Let f be a continuous function defined on the interval $[a, b]$ and let be any number strictly between $f(a)$ and $f(b)$. Then there exists a number $c \in (a, b)$ such that $f(c) = q$.

3.3 Proof by Contradiction

Suppose you want to prove Q. Assuming $\neg Q$, we follow logical conclusions to arrive at a falsehood. This means $\neg Q$ cannot be true, so Q is true.

Example. Prove that Tuesday is not three days before Thursday.

Proposition. There does not exist a number $x \in \mathbf{Q}$ such that $x^2 = 2$. (That is, $\sqrt{2}$ is an irrational number.)

Proof.

If we are trying to prove $P \Longrightarrow Q$ by contradiction, we assume $\neg(P \Longrightarrow Q) \equiv P \wedge \neg Q$.

Example. Suppose a function f is continuous on the interval (a, b). If $f(x) \neq 0$ for all $x \in (a, b)$, then $f(x_1)$ and $f(x_2)$ have the same sign for every $x_1, x_2 \in (a, b)$.

Note. Trying to prove $P \Longrightarrow Q$ by contradiction, we assumed $P \wedge \neg Q$. Then we arrived at $\neg P$ without using the assumption P, which means we actually proved $\neg Q \Longrightarrow \neg P$, the contrapositive.

In general, it is better to prove the contrapositive $\neg Q \Longrightarrow \neg P$ (if it is not too hard to understand) than to use a contradiction that assumes $P \wedge \neg Q$ and arrives at Q without using P.

Proposition. Let $a, b \in \mathbf{R}$. If $a < b$, then $\dfrac{a+b}{2} < b$.

Try proof by contradiction:

Logical basis for proof by contradiction

Proof by contradiction is based on the tautology $(\neg Q \implies F) \implies Q$. We show it is a tautology.

$(\neg Q \implies F) \implies Q =$

Another way to look at it: $\neg Q \implies F$ is only true if $\neg Q$ is false.

3.4 Using Cases in Proofs

When proving a statement, sometimes it helps to break the proof into cases for the variable.

Example. Show that $3n^2 - 7n + 24$ is an even integer for all integers n.

Cases often come up when proving statements about absolute value. Recall that

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

Theorem. Let $a \geq 0$. Then
1) $|x| = a$ if and only if $x = a$ or $x = -a$
2) $|-x| = |x|$

Proof.

Theorem. Let $a \geq 0$. For all $x, y \in \mathbf{R}$, we have
1) $|x| \leq a$ if and only if $-a \leq x \leq a$
2) $|xy| = |x||y|$
3) $|x + y| \leq |x| + |y|$ (triangle inequality)

Proof.

3.5 The Division Algorithm and Congruence

We have seen how to divide integers with remainder:

$$56 \div 9 = 6, \text{ remainder } 2, \text{ which means that } 56 = 6 \cdot 9 + 2$$

We have a general statement about division with remainder.

Theorem (The Division Algorithm). Let $n > 0$. For every integer a, there exist unique integers q and r, $0 \leq r < n$ such that $a = q \cdot n + r$.

"Proof."

Theorem. Let $a \in \mathbf{Z}$ and $n \in \mathbf{N}$.
1) If $a = nq + r$, then $a \equiv r \pmod{n}$.
2) a is congruent to a unique integer n such that $0 \leq r < n$.

Proof.

Example. Fill in the table so that $0 \leq r < 7$.

a	$a \equiv r \pmod{7}$
3	
22	
45	
-33	
-16	

Example. For every $a \in \mathbf{Z}$, $a^3 - a$ is divisible by 3.

Theorem. Let $n \in \mathbf{N}$ and $a, b, c, d \in \mathbf{Z}$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
1) $a + c \equiv b + d \pmod{n}$
2) $ac \equiv bd \pmod{n}$
3) $a^m \equiv b^m \pmod{n}$ for every $m \in \mathbf{N}$

Proof. 1) and 2) were done for homework, and 3) immediately follows from 2).

Example. Use the above theorem to easily prove the previous statement: for every $a \in \mathbf{Z}$, $a^3 - a$ is divisible by 3.

Proposition. For all $a, b \in \mathbf{Z}$, if $5 \mid ab$, then $5 \mid a$ or $5 \mid b$.

Example. Try to prove this statement with the method above:
for all $a, b \in \mathbf{Z}$, if $6 \mid ab$, then $6 \mid a$ or $6 \mid b$.