Methods of Proof

Given a mathematical statement, we want to directly reason to a resolution of whether the statement is true or false, i.e., to <u>prove</u> or <u>disprove</u> the statement. Sometimes this is impossible or unclear!

Contradiction

Given a statement, assume its negation. Reason from this assumption to a conclusion you know to be false. Therefore, the original statement must be true!

Example 1: There are infinitely many prime numbers.

proof: By contradiction. Suppose there are finitely many prime numbers $p_1, p_2, p_3, \ldots, p_n$.

Let

$$x = (p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n) + 1.$$

Dividing x by any of the primes $p_1, p_2, \ldots, p_n$ yields a remainder of 1.

We have two possibilities:

either

1) x is prime, which immediately contradicts our assumption that there are n primes, or

2) x is composite, which implies the existence of a prime that divides x that is not equal to any of $p_1, p_2, \ldots, p_n$. This is again a contradiction.

Therefore, we must have infinitely many primes.

$\square$

Remark: (the contrapositive)

Recall that the contrapositive of an implication "if P, then Q" is the logically equivalent statement "If not Q, then not P". Every proof by contradiction can be reworded as a proof of the contrapositive, but is often more difficult to write!

Open Problem: the Twin Prime conjecture!

We know there are infinitely many prime numbers. Do there exist infinitely many prime numbers p such that $p+2$ is also a prime number?

Conjecture: Yes! But no one can prove it...

Induction

A bootstrap method for proving statements $P(n)$ indexed by the natural numbers. The idea is:

base step → 1) Establish $P(1)$ to be true.

inductive step → 2) Assume $P(n)$ to be true for an arbitrary natural number n, $n \geq 1$. Prove that, under this assumption, $P(n+1)$ is true.

Combining these steps proves $P(n)$ for all natural numbers n.

Example 2: Let $p(x)$ be a nonconstant polynomial with complex coefficients and suppose $p(x)$ has a root in $\mathbb{C}$.

a complex number

$P(n)$ Then if the degree of $p(x)$ is n, $p(x)$ factors into a product of linear terms, and thus has n roots (possibly repeated) in $\mathbb{C}$.

proof: Use induction: Start with $n=1$. Then $p(x) = ax+b$ for some $a, b \in \mathbb{C}$ and is already linear.

Before the general proof, let's see how to get from n to $n+1$ with some values of n.

$n=2$: Then $p(x) = ax^2 + bx + c$ where $a \neq 0$. We assume that $p(x)$ has a root in $\mathbb{C}$, and therefore, denoting this root by α, $(x-\alpha)$ divides $p(x)$. But $p(x)$ is quadratic, so

$$p(x) = (x-\alpha)(ax+d)$$ for some $d \in \mathbb{C}$, and hence factors linearly.

$n=3$: Then $p(x) = ax^3+bx^2+cx+d$ with $a \neq 0$. Then by assumption, $p(x)$ has a root $\alpha \in \mathbb{C}$, so $(x-\alpha)$ divides $p(x)$. But $p(x)$ is cubic, so

$\boxed{p(x) = (x-\alpha)\, q(x)}$ where the degree of $q(x)$ is 2.

By the $n=2$ step, $q(x)$ factors linearly, and so $p(x)$ factors linearly

General n: Our inductive step is to assume that, for a natural number $n \geq 2$, that every polynomial of degree $n-1$ factors linearly. Now suppose $p(x)$ has degree n. By assumption, $p(x)$ has a root $\alpha \in \mathbb{C}$, so again, $(x-\alpha)$ divides $p(x)$. We may then write

$$\boxed{p(x) = (x-\alpha)\,q(x)}.$$

By the inductive hypothesis, $q(x)$ factors linearly and therefore $p(x)$ factors linearly.

Our general statement is then true due to induction.

Remark: The fact that every polynomial with complex coefficients that is nonconstant has a complex root is called the **Fundamental Theorem of Algebra**.

The proof of this result appears to always involve mathematics other than algebra!

(Take Complex Variables, Math 455)

Remark: (the well-ordering principle)

The Well-Ordering Principle states that every nonempty subset of the natural numbers has a least element. This principle is equivalent to the fact that induction works (the Principle of Mathematical Induction)

The Well-Ordering Principle is not to be confused with the Well-Ordering Theorem, which states that any set can be well-ordered. The Well-Ordering Theorem is equivalent to the Axiom of Choice!

Proof by Cases

(Exhaustion)

Take a statement you want to prove. Divide into n subcases. Prove each subcase.

Example 3:

The triangle inequality for real numbers:

if $x, y, z \in \mathbb{R}$, then

$$|x-z| \leq |x-y| + |y-z|.$$

proof: By cases. Let $a = x-y$, $b = y-z$. We reduce to proving

$$\begin{aligned} |a+b| &= |x-y+y-z| \\ &= |x-z| \\ &\leq |x-y| + |y-z| \\ &= |a| + |b|. \end{aligned}$$