THEOREMS AND PROOFS

PENN SUMMER PREP PROGRAM
EXPLORATIONS IN MATHEMATICAL INQUIRY

MATT DECROSS

The content of nearly all mathematics papers consists of a set of assertions ("theorems") along with a series of arguments showing that they are true (a "proof"). The idea is that these arguments should start with some set of accepted truths and make a series of incontrovertible statements that end in the conclusion that the original assertion is true. In school, you may have learned about this idea of "theorems" and "proofs" through the framework of the "two-column proof," with assertions drawn from Euclidean geometry or basic logic. While this framework captures the idea of logical flow from one idea to another, the assertions are often too simplistic, the arguments too obvious, and the structure (of two columns) too rigid and formal for easy reading of more complicated proofs.

In this assignment, we introduce several important basic proof techniques and examples of assertions easily proved with them. For each assertion, try to write up a proof that it is true. This may be difficult, and I don't intend for it to be overly time-consuming, so feel free to instead look up the proofs after trying each for a bit (each assertion and its proof are well-known), understand them, and then write up your own versions instead. That being said, it is also useful to try several approaches and learn what *doesn't* work, which can often provide the insight/perspective on how to approach a problem. Rather than the two-column format, your proofs should generally be written in a paragraph format, with equations interspersed, along the same lines as the examples.

Due Thursday on paper.

Direct Proof

Direct proofs are the most straightforward, as the name would imply. Simple direct proofs often proceed by expanding definitions of terms and using different ways of expressing formulas until it is clear that the claim is true. More complex direct proofs may have many steps and define new symbols and variables, but the general logical flow is the same: proceed linearly from claim to claim; do not pass go.

Example

The below theorem is called *Euclid's formula*:

Theorem.
Given an arbitrary pair of positive integers m and n with $m > n$, the integers $a = m^2 - n^2$, $b = 2mn$, and $c = m^2 + n^2$ form a Pythagorean triple.

Proof.
Squaring the relevant integers:

$$a^2 + b^2 = (m^2 - n^2)^2 + (2mn)^2 = m^4 + n^4 - 2m^2n^2 + 4m^2n^2 \tag{1}$$

$$= m^4 + n^4 + 2m^2n^2 = (m^2 + n^2)^2 = c^2 \tag{2}$$

So $a^2 + b^2 = c^2$, the Pythagorean theorem, holds for the integers a, b, and c defined as above. $\square$

Problems

(1) Prove that $3n(n^2+n+1)+(1-n)(n^2+n+1)-n^3$ is a perfect cube for all positive integers n. (Hint: As shown in problem (5), $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$).

Proof by Contradiction

The idea of a proof by contradiction is to first start by assuming the *opposite* of what you want to prove. Then, show that this leads to a statement that you already know to be false. Therefore, the opposite of what you want to prove is false. So, what you want to prove is true. It is often a good idea to use this proof method when it's hard to say anything concrete about a statement, but easy to say something concrete about the opposite of a statement, as in the below example.

Example

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

Proof.
We proceed by contradiction. Assume $\sqrt{2}$ were rational. Then $\sqrt{2}$ can be represented as a fraction in simplest form, so there exist positive integers p, q that share no common factors such that:

$$\sqrt{2} = \frac{p}{q}. \tag{3}$$

Squaring both sides of (3) and rearranging, we have

$$p^2 = 2q^2. \tag{4}$$

The right-hand side above is even, so p must be even since any odd number squared is still odd. So we can write $p = 2n$ for some positive integer n that shares no common factors with q, and (4) becomes:

$$4n^2 = 2q^2 \implies q^2 = 2n^2. \tag{5}$$

This implies q^2 and q are both even. But then both p and q are even, so they both share at least a common factor of 2. This contradicts the claim that p, q share no common factors; thus, no such representation $\sqrt{2} = p/q$ exists i.e. $\sqrt{2}$ is irrational. $\square$

Problems

(2) Prove that $\sqrt{p}$ is irrational for any prime p. (Hint: you can use an argument similar to the above. Or, for a more refined approach, use the Fundamental Theorem of Arithmetic, which says that every natural number ≥ 2 has a unique prime decomposition).

(3) Prove that there are infinitely many prime numbers. (Hint: you'll need to construct a larger prime from finitely many primes or show that there exists a larger number which isn't prime but no smaller prime divides it).

Proof by Induction

Proofs by induction are typically catered to statements that you want to prove for all natural numbers n - when you see a statement that's indexed by such a number, it's usually the first thing you want to think of trying. A proof by induction proceeds in several steps. First, you prove whatever it is you want to prove for a "base case," such as $n = 1$. Then, you assume the statement is true for some natural number $n - 1$, and try to show that it's true for n *given that* it's true for

$n-1$ (the "inductive hypothesis"). Having established the base case, this proves the claim for all natural numbers (since then you have that it's true for $n=1$, and if it's true for $n=1$ then it's true for $n=2$, and if it's true for $n=2$ it's true for $n=3$...).

Example

Theorem.
The sum of the first n positive integers is

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \tag{6}$$

Proof.
When $n=1$, we have $\sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2}$, so the base case $n=1$ is established. Assuming the theorem is true for $n-1$, we can write the left-hand side of the theorem as

$$\sum_{k=1}^{n} k = \sum_{k=1}^{n-1} k + n = \frac{(n-1)n}{2} + n = n + \frac{1}{2}n^2 - \frac{1}{2}n = \frac{n(n+1)}{2} \tag{7}$$

where in the second equality we used the inductive hypothesis. □

Problems

(4) Prove that the sum of the first n perfect squares is

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}. \tag{8}$$

(5) Prove the binomial theorem for all positive integers n,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k. \tag{9}$$

Note: recall that $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is the number of ways of choosing a subset of k objects from a set of n objects, with $n! = n \times (n-1) \times \ldots \times 1$. These are also the binomial coefficients or the numbers in Pascal's triangle; remember that they satisfy the relation $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$.

Proof of Uniqueness

In a uniqueness proof, one must show that some object is the *only* object with a desired property. A typical method of proving uniqueness is to assume first that the object is *not* unique; rather, assume there are two objects with the desired property. Then, show that both objects must actually be the same object. Thus, there was only one object all along. Another possibility is to explicitly construct the object from the desired properties and to show that the object is uniquely fixed by the properties.

Example

Theorem.
For all real numbers x and y with $x \neq 0$ there exists exactly one real number a such that $ax+y=0$.

Proof.
We notice that $a = -\frac{-y}{x}$ solves the equation, so there does exist one such real number. Let b be another such real number that solves the above equation. Then $ax + y = 0$ and $bx + y = 0$, so $ax + y = bx + y \implies ax = bx \implies a = b$ since x is nonzero. Thus, a is unique. □

Problems

(6) Prove that the empty set is unique. Note that two sets are defined to be equal if each is a subset of the other, and a set is defined to be a subset of another set if all of its elements are contained in it.

Proof by Construction

A construction proof is exactly what it sounds like - to demonstrate that something exists with some desired property, you can just construct something with the property. This is the "easy" version of an existence proof - sometimes it is true that something exists but impossible or very difficult to construct it!

Example

Theorem.
Show that there exists a line in the Cartesian plane of slope 2 *that intercepts the* y *axis at* $y = 4$.

Proof.
Consider the general equation for a line in the Cartesian plane, $y = mx + b$. When $x = 0$, we have that $y = 4$, so $b = 4$. The slope is the difference in y values between two points divided by the difference in x values:

$$\frac{y_2 - y_1}{x_2 - x_1} = \frac{mx_2 + b - mx_1 - b}{x_2 - x_1} = \frac{mx_2 - mx_1}{x_2 - x_1} = m \tag{10}$$

so $m = 2$ is the slope. Thus, $y = 2x + 4$ is the equation of such a line. □

The above proof is actually also a uniqueness proof, since we showed that the desired properties of the line fix all of the free constants that determine the equation of a line.

Problems

(7) Prove that for any positive integer n, there exists a prime number p_1 such that if p_2 is the next largest prime greater than p_1, then $p_2 - p_1 \geq n$. (Hint: you don't need to construct p_2. Given a prime p_1, can you show that there exists a sequence of consecutive composite numbers whose length must be close to that of p_1? Then, using the fact that the primes get arbitrarily large, you would be done).

Proof by Counterexample

Proofs by counterexample are one of the easiest forms of (dis)proofs. This is because rather than providing a long formal argument, this kind of proof usually just points out a case that other people hadn't seen before. A proof by counterexample might be used to prove a theorem of the form "No object with property X" exists by demonstrating an object with property X.

Example

This example is a famous conjecture of Euler, disproved in the paper: Lander, L. J., and Parkin, T. R. (1966) Bulletin of the American Mathematical Society, 72(6), 1079.

Theorem.
It is false that at least n nth powers are required to sum to an nth power when $n > 2$.

Proof.
A counterexample is $27^5 + 84^5 + 110^5 + 133^5 = 144^5$, which is a sum of 4 5th powers summing to a 5th power. □

Problems

(8) Provide a counterexample to the following claim: all two-digit prime numbers are within 5 of the closest prime to themselves.

Proof by Contrapositive

This proof method is not really distinct from direct proof since it is logically equivalent, but it is useful to remember as a separate technique. The idea is that if you want to show $P \implies Q$, it's equally logically valid to show that $\neg Q \implies \neg P$, where $\neg$ means the negation of the statement P or Q. Usually the contrapositive is just a rephrasing that conveniently allows you to use some concrete facts that you already know.

Example

Theorem.
Prove for any positive integer n that if n^2 is odd, then n is odd.

Proof.
We will show that if n is not odd, then n^2 is not odd. If n is not odd, then it is even and we can write it as $n = 2k$ for some positive integer k. Then $n^2 = (2k)^2 = 4k^2$. But this contains 2 as a factor, so n^2 is even and not odd. □

Problems

(9) Suppose x and y are real numbers such that the product xy is irrational. Prove by contrapositive that at least one of x and y is irrational.