Section 3.1: Direct Proof and Counterexample 1

In this chapter, we introduce the notion of proof in mathematics. A mathematical proof is valid logical argument in mathematics which shows that a given conclusion is true under the assumption that the premisses are true. All major mathematical results you have considered since you first started studying mathematics have all been derived in this way e.g. Pythagoras Theorem, Fundamental Theorem of Calculus, Fundamental Theorem of Algebra. Most of these proofs are long and complicated and will be considered in further mathematics courses. In this course, we shall consider more elementary proofs, mainly in number theory, to start and strengthen our proof writing abilities.

1. Definitions

As stated at the beginning of the course, one of the most important parts of mathematical proof is knowing and understanding the definitions of what you are trying to prove things about. In this class **and all future classes** if you do not learn and understand the definitions **you will not** be able to prove things. Again, just for emphasis, **definitions are one of the most important parts of a mathematical proof**. For a comparison, you wouldn't write an essay using words which you don't know what they mean, so why would you try to write a mathematical proof about things you don't understand?
As remarked above, in this chapter, we shall be considering a number of different proofs in number theory, so we start by writing formal definitions. Note that none of the definitions we are going to write down are new to us, but the formal definition probably is.

Definition 1.1. (Odd and Even Integers) An integer n is even if and only if $n = 2k$ for some integer k. An integer is odd, if and only if $n = 2k + 1$ for some integer k. Symbolically:

$$\forall n \in \mathbb{Z}, n \text{ is even} \iff \exists k \in \mathbb{Z}, n = 2k$$

$$\forall n \in \mathbb{Z}, n \text{ is odd} \iff \exists k \in \mathbb{Z}, n = 2k + 1$$

Definition 1.2. (Prime Numbers) An integer n is prime if and only if $n > 1$ and for all positive integers r and s, if $r \cdot s = n$, then $r = 1$ or $s = 1$. An integer n is composite if and only if $n > 1$ and $n = r \cdot s$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$. In formal notation:

$$\text{n is prime} \iff \forall r \in \mathbb{Z}^+, \forall s \in \mathbb{Z}^+, n = r \cdot s \to (s = 1 \vee r = 1)$$

n is composite $\iff \exists r \in \mathbb{Z}^+, \exists s \in \mathbb{Z}^+, (n = r \cdot s) \wedge ((s \neq 1) \wedge (r \neq 1))$

Notice that definitions are $\iff$ statements i.e. quantified biconditional statements. We consider some examples of how to use these definitions.

Example 1.3. Use the definitions we have given to answer the following:

(*i*) Is 5 odd?

5 is odd if 5 can be written in the form $2k + 1$ for some integer k. Let $k = 2$. Then $5 = 2 \cdot 2 + 1$, and thus by definition 5 is odd.

(*ii*) Is $nm - m$ composite for $n > 2$ and $m > 1$.

$nm - m$ is composite if $nm - m = r \cdot s$ for some integers $r, s > 1$. However, $nm - m = m(n - 1)$, so if we choose $r = m$ and $s = n - 1$, then $nm - m = r \cdot s$ where $r, s > 1$, so by definition, $nm - m$ is composite.

(*iii*) Is $2r - 6 + 10s$ even?

$2r-6+10s$ is even if $2r-6+10s2 \cdot k$ for some integer $k > 0$. If we choose $k = (r - 2 + 5s) > 0$, then $r - 2 + 5s > 1$ and $s = n-1$, then $nm-m = r \cdot s$ where $r, s > 1$, so by definition, $nm - m$ is composite.

2. Proving and Disproving Existential Statements

Arguably, the easiest statements to prove are existential statements i.e. statements of the form

$$\exists x \in D, Q(x)$$

or "there exists x such that $Q(x)$ is true". In order to prove such statements, we need to exhibit an explicit example of $x \in D$ with property Q (or such that $Q(x)$ is true), or describe a set of directions in order to find such an x. These methods of proof are called "constructive proofs", as opposed to non constructive proofs where the existence of an element is guaranteed by an axiom, or previous proof, or is proved by contradiction (by assuming such an x does not exist). We illustrate with some examples.

Example 2.1. Show that there exists two prime numbers n and m such that $n + m = 18$.

Choose $n = 7$ and $m = 11$, then $n + m = 11 + 7 = 18$.

Example 2.2. Suppose that k is an even integer and $k > 2$. Show that there exists two prime numbers n and m such that $n + m = k$.

(Goldbachs conjecture!!!!)

Example 2.3. Show that there exists real numbers a and b such that $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$.

Take $a = 0$ and $b = 1$. Then

$$\sqrt{0+1} = \sqrt{1} = \sqrt{0} + \sqrt{1}$$

To disprove an existential statement, we need to prove its negation i.e. to disprove an existential statement, we need to prove the universal statement which is the negation of the existential statement. Since we shall be considering universal statements until later, we shall return to this problem then.

3. Disproving a Result by Counterexample

To disprove a statement means to show it is false. One typical way to disprove a universal statement is to present a counterexample to what is being posed. Formally:

Result 3.1. (Disproof by Counterexample) To disprove the universal statement

$$\forall x, P(x) \to Q(x)$$

means to find an x such that $P(x)$ is true, but $Q(x)$ is false. In notation,

$$\exists x, P(x) \wedge \sim Q(x).$$

We call such an x a counterexample.

Example 3.2. Consider the statement "for all real numbers x, if x^2 is rational, then x is rational". Disprove this statement by giving a counter example.

Consider the number $x = \sqrt{2}$. Clearly $\sqrt{2}^2 = 2$ is rational. However, $\sqrt{2}$ is not rational (we shall see why later in the course). Thus we have exhibited a real number x such that x^2 is rational but x is not rational, and thus the universal statement is not true.

4. Proving Universal Statements

Some of the most difficult statements to try to prove (and usually the most interesting and useful statements to try to prove) are universal conditional statements i.e. statements of the form

$$\forall x \in D, P(x) \to Q(x).$$

The first obvious way to attempt to prove such a statement is the following:

Result 4.1. (Method of Exhaustion) When the domain D of x is finite, to prove the universal statement

$$\forall x \in D, P(x) \to Q(x)$$

we can simply check for every element in D that if $P(x)$ is true, then so is $Q(x)$.

It seems that the method of exhaustion is the best way to prove universal conditionals. However, it has one huge obstacle - it only works for finite sets! (and in math, we are nearly always considering statements about infinite sized sets). Therefore, in general, we would try a method more like the following:

Result 4.2. (Method of Direct Proof) Suppose you are trying to prove a universal conditional statement. Then we do the following:

(*i*) Express the expression in logical form i.e. identify the hypothesis and conclusion of the statement and the domain.
(*ii*) Start the proof by supposing that x is a particular, but arbitrary chosen element of D for which $P(x)$ is true.
(*iii*) Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules of logical inference.

The last two steps are sometimes called "The method of generalizing from the generic particular".

We illustrate these proof techniques with a couple of examples.

Example 4.3. For each integer n with $1 \leqslant n \leqslant 5$, $n^2 - n + 11$ is prime.

Since there are only finitely many integers with $1 \leqslant n \leqslant 5$, we can use the method of exhaustion. Specifically, we have

$$1^2-1+11 = 11, 2^2-2+11 = 13, 3^2-3+11 = 17, 4^2-4+11 = 23, 5^2-5+11 = 31.$$

In each case, the resulting number is prime, so the statement is true.

As remarked before, proving universal statements with infinite domains is much more difficult. The following three steps will usually help with such problems:

(*i*) (Formal Restatement) Always try to write a formal restatement of the theorem you are trying to prove i.e. transform the statement from informal language to logic.
(*ii*) (Starting Point) Write down the things you are allowed to assume given the statement of the theorem i.e. to prove a statement $\forall x, P(x) \to Q(x)$, you need to suppose x is an arbitrary object which makes $P(x)$ true, and then show that $Q(x)$ is true. For example, in the last problem we considered, the starting point was the assumption that x was odd.
(*iii*) (The Conclusion) Always keep in mind what the conclusion is going to be. Sometimes, it may even be useful to have it written somewhere on the page so you have a "roadmap" of where you want to go.

Example 4.4. Show that for any integer n, if n is odd, then n^2 is odd.

In this case, we cannot use the method of exhaustion since there are infinitely many different odd integers. Therefore, we must use the method of generalizing from the generic particular. Specifically, assuming that x is an odd integer, we need to show that without any further assumptions that x^2 is odd. We shall follow the steps above.

(*i*) (Formal Restatement) $\forall x \in \mathbb{Z}, x$ is odd $\rightarrow x^2$ is odd
(*ii*) (Starting Point) Our only assumption is that x is some odd integer. This means that $x = 2k + 1$ for some integer k.
(*iii*) (Body) Since $x = 2k+1$, we have $x^2 = (2k+1)^2 = 4k^2+4k+1$ (using standard rules of algebra). Therefore, if $m = 2k^2 + k$, then $x^2 = 2m + 1$.
(*iv*) (Conclusion) Therefore x^2 is an odd integer

5. General Proof Techniques and Common Mistakes

A large portion of this class will be dedicated to learning how to write mathematical proofs of statements (we usually call such statements "Theorems"). There is a widely accepted structure to such communication, so we shall briefly outline how you should present your proofs. In addition, there are some useful general steps and techniques which should always be taken when writing a proof, and also some common pitfalls which people fall into when writing proofs. First, when trying to prove a theorem, the general structure should be as follows:

(*i*) Write the word "Theorem" and then the statement you are trying to prove after it.
(*ii*) On the next line write the word "proof" - it is from this point onward you shall start to write your proof. Note that this separates the statement of the theorem from the proof, so should help avoid any confusion.
(*iii*) Clearly mark the end of your proof with "QED", or some other such symbol (this is especially important if you are proving three or four statements.

In addition to the general structure given above, a good (and correct!) proof will exhibit the following:

(*i*) A proof should always be self-contained, meaning all variables which are used in the proof should be clearly defined
(*ii*) You should write a proof in complete sentences. This doesn't mean you should not use symbols or abbreviations in a proof, but rather they should be incorporated into your sentences
(*iii*) Provide a reason for each assertion you make in you proof or each step you take - if you don't back up the steps you take, you could end up assuming something that isn't true.

(*iv*) Use typical "buzzwords" between statements to make the argument in your proof more clear. For example, if one statement is a consequence of the previous, we could use the word "therefore", or "it follows that" with a brief reason why the second statement follows from the first at the end of the sentence. When introducing new variables, we use the word "let" (e.g. let x be an even integer).

As usual, there are certain mistakes which beginners (and indeed experts) make when writing proofs. Some of the more common ones you should watch out for are the following:

(*i*) Trying to prove a universal statement through examples: remember, just because a statement holds for a small number of examples, does not mean it holds for all examples!
(*ii*) Using the same variable to represent more than one thing
(*iii*) Jumping to a conclusion i.e. asserting the truth of a statement without giving a reason
(*iv*) Begging the question i.e. assuming what you are trying to prove
(*v*) Misuse of the word "if" i.e. "if" can sometimes be used instead of the word "because", so a statement which is meant to be an assertion can turn out to be conditions because the word "if" is used instead of because.

We illustrate with a formal proof.

Example 5.1. Prove the statement "The difference of any two odd integers is even"

Theorem 5.2. *The difference of any two odd integers is even or*

$$\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x \text{ is odd} \wedge y \text{ is odd} \rightarrow x - y \text{ is even}$$

Proof. Suppose x and y are (arbitrary but particular) odd integers. Then there exists an integer k such that $x = 2k + 1$ and an integer m such that $y = 2m + 1$. Taking the difference of x and y, we get

$$x - y = 2k + 1 - (2m + 1) = 2k + 1 - 2m - 1 = 2k - 2m = 2(k - m)$$

use the standard rules of arithmetic. In particular, $x - y = 2(k - m)$ and $k - m$ is an integer. Therefore, $x - y$ is even.

□

We finish with an example.

Example 5.3. Check to see if the following statement seems true or false and then prove or disprove accordingly: "There exists an integer $m \geqslant 3$ such that $m^2 - 1$ is prime" is false.

Looking at a small number of examples, we do not get any primes, so our gut feeling is that this should be false. In order to show that this statement is false, we need to show the negation is true.

Theorem 5.4. *$\forall m \in D, m^2 - 1$ is not prime where D is the set of all integers greater or equal to* 3*.*

Proof. Suppose $m \in D$. Using simple algebra, $m^2 - 1 = (m-1)(m+1)$. Since m is an integer, so are $m-1$ and $m+1$. Since $m \geqslant 3$, $m-1 \geqslant 2$ and $m+1 \geqslant 2$. In particular, $m^2 - 1$ is the product of two positive integers greater than 1 and hence by definition, it is not prime. □

Homework

(*i*) From the book, pages 139-141: Questions: 2, 7, 11, 14, 21, 25, 32, 36, 42, 46, 47