P.11 More on Proof

Believe it or not, we've actually covered all of the fundamental proof techniques. Any statement of the form "If P, then Q" can be proved using direct proof, contrapositive proof, or contradiction proof (assuming the statement can be proven at all). We will devote the remainder of the semester to writing proofs of particular kinds of statements. Often, we will still employ one of the methods mentioned above, but there are certain expectations and conventions for these types of proofs that we will follow.

Goals:

- Write Biconditional Proofs
- Prove Existence Theorems

1 Biconditional Proofs

Recall that a biconditional statement has the form $(P \Leftrightarrow Q)$, which is read as "P if and only if Q". This is really just short hand for $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. To prove a biconditional statement we must prove both $P \Rightarrow Q$ and its converse $Q \Rightarrow P$. In other words, we have to write two proofs in one. Generally speaking, the two pieces may require two different proof techniques. It is very common that $P \Rightarrow Q$ can be done via direct proof, but $Q \Rightarrow P$ requires proof by contrapositive or contradiction.

1. Follow the steps below to prove the following claim.

   Claim 1. The integer n is even if and only if n^2 is even.

   (a) Determine the two conditional statements that comprise the conditional statement in the claim.

   (b) Prove the first conditional statement using any means you find appropriate.

(c) Prove the second conditional statement using any means you find appropriate.

(d) Combine the two proofs to prove the biconditional statement. Yes, I'm requiring that you write out everything again. Keep the following in mind: (1) the proofs of the two conditional statements must be in separate paragraphs, and (2) the second paragraph should begin with "Conversely," to indicate that you're proving the converse of the first statment. When we are writing biconditional proofs by hand, we often label the two directions with "($\Rightarrow$)" and "($\Leftarrow$)." This is usually considered inappropriate in formal proof writing, but it's a good idea while you try to get used to the technique.

2. Prove the following biconditional statement.

   Claim 2. Suppose $a, r \in \mathbb{Z}$, $n \in \mathbb{N}$, and $0 \leq r < n$. Then $a \equiv r (\text{mod } n)$ if and only if a has remainder r when divided by n.

Other than the fact that you have to write two proofs in one, there's really nothing new to you about writing biconditional proofs. Therefore, we'll move on to something that is new.

2 Equivalent Statements

If the statement "P if and only if Q" holds, then we often refer to P and Q as equivalent statements. This is because if we know that one is true then we can automatically assume that the other is also true. There are many very important theorems in math (especially in linear algebra) that are really just a list of equivalent statements. The example below gives such a list (this example is not from linear algebra).

Claim 3. The following statements are equivalent.

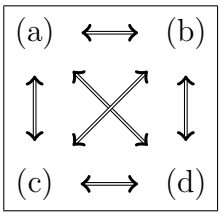
(a) The integer n is even.

(b) The integer n^2 is even.

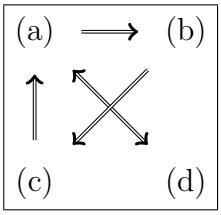
(c) The integer n^3 is even.

(d) The integer n^2 is divisible by 4.

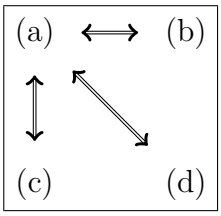
Again, by equivalent the claim means the biconditional statements $(a) \Leftrightarrow (b)$, $(a) \Leftrightarrow (c)$, $(b) \Leftrightarrow (c)$, and (c) $\Leftrightarrow$ (d) are all true. The diagram below shows the relationships between the statements.



In reality, this diagram is equivalent to the one below. If we wanted to prove the claim, it would be easiest to prove the relationships as described in the following diagram because it would require fewer proof directions.



Unfortunately, proving $(b) \Rightarrow (c)$ would be difficult, so we would have to prove this claim according to the following diagram. It requires six proof directions, but it's still the easiest way to go.



We won't actually write any equivalent statement proofs this semester. They only employ the methods we know, so ultimately they just take longer than the proofs we write otherwise. Still, you should be aware of them and prepared to see them in future courses.

3 Existence Proofs

Thus far we've only proved statements of the form $P \Rightarrow Q$. Even biconditional statements amount to proving this type of statement. We move now to proving "existence" statements. Existence statements are statement that claim that some entity exists. They take the form

$$\exists\ x,\ P(x).$$

Recall that in the above notation, P is a statement whose truth value depends on the value of x. Proving existence statements is actually quite simple in concept. All we have to do is give an example of the thing that's supposed to exist. Of course, our proof should also include an explanation of why our example fits the requirements of the claim.

Claim 4. There exists a smallest odd prime number.

Proof. The smallest odd prime number is 3. Notice that $3 = 2(1) + 1$ so 3 is odd. Also, the only natural numbers that divide 3 are 1 and 3. Finally, the odd prime numbers are a subset of the natural numbers so the Well-Ordering Principal guarantees the existence of a smallest element. Since the only natural numbers less than 3 are 1 and 2, 1 is not prime, and 2 is not odd, we know that 3 is the smallest odd prime number. □

The proof above is considered a **constructive** proof. This is because it proves that statement and constructs (or in this case provides) the smallest odd prime number. The proof below is **non-constructive**. It ensures that the smallest odd prime exists, but does not provide it.

Proof. Notice that all prime numbers are natural numbers, so the odd prime numbers are a subset of the natural numbers. As such, the Well-Ordering Principal guarantees the existence of a least element. □

It probably does not surprise you that constructive proofs are often preferred since the provide an example. However, both are acceptable in general.

3. Prove the following existence statements.

   Claim 5. There exists a positive real number x for which $x^2 < \sqrt{x}$.

Claim 6. There exist distinct irrational numbers a and b such that ab is rational.