Basic Existence Proofs

Many definitions in mathematics involve existence statements. In some sense the most fundamental piece of proof writing is showing that an element of a set satisfies some definition. Doing so requires what is called an existence proof.

> Goals:
>
> - Write existence proofs based on given definitions

Why you're here: You're in this course to learn to write mathematical proofs of statements. To make this a digestible task, you'll be writing proofs of statements that we already know to be true. You will often think to yourself "Isn't that obvious?" Maybe it is, but that doesn't mean you don't have to prove it. If a statement isn't an axiom then it needs to be proven. Once it has been proven it can be used in the future.

You need to master the art of proof writing before you move on to more advanced math courses. Abstract Algebra and Real Analysis are difficult enough on their own. If you're trying to digest material from these courses and figure out how to write proofs in them at the same time, then you won't be successful.

We will need the following definitions for this topic and throughout the remainder of the semester.

Definition 1 (Even) An integer n is **even** if there exists $k \in \mathbb{Z}$ such that $n = 2k$.

Definition 2 (Odd) An integer n is **odd** if there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$.

Definition 3 (Divides) An integer a **divides** an integer b, denoted $a \,|\, b$, if and only if there exists $k \in \mathbb{Z}$ such that $ak = b$.

Note: The expression "$a \,|\, b$" is a mathematical statement, not a mathematical expression. That is, "$a \,|\, b$" is true or false. Do not confuse this notation with the expression "a/b" which is a rational number.

If $a, b \in \mathbb{Z}$ and $a \mid b$, then we will often say that b is a **multiple** of a. For instance, "$5 \,|\, 10$" and "10 is a multiple of 5" give us the same information. The terms "divides" and "multiple" can be used in similar situations, but "divides" tends to be more concise. For instance, consider

$$\{k \in \mathbb{N} : k \,|\, 12\} = \{k \in \mathbb{N} : 12 \text{ is a multiple of } k\} = \{1, 2, 3, 4, 6, 12\}.$$

Writing note: The word "divides" is an active verb, where as "is" is not. Most of us naturally prefer action verbs when reading. As a result, saying "$5 \,|\, 10$" instead of "10 is a

multiple of 5" will make your writing more interesting to read.

Consider the statement P:"The integer 6 is even." Odds are that you're willing to accept this statement as being true without any argument. You've been exposed to even and odd integers for some time now. Still, this example will serve as great practice.

The statement P is an existence statement in disguise.

$$P \equiv Q : \text{"There exists an integer } k \text{ such that } 6 = 2k.$$

While statements P and Q say exactly the same thing, Q helps us understand what we need to do to demonstrate that P is true: we need to provide and integer k so that $2k = 6$. The integer 3 should work just fine.

Claim 1. *The integer 6 is even.*

Proof. Notice that $2(3) = 6$, so there exists an integer k such that $6 = 2k$. Thus 6 is even by definition. □

Directions: Prove the following existence statements. Please note that being asked to prove something means you're being asked to do more than provide the example for the existence statement. You need to use full sentences and reference appropriate definitions and axioms.

Claim 2. *The integer 8 is even.*

Claim 3. *The integer 7 is odd.*

Claim 4. *The integer -5 is odd.*

Claim 5. *The integer 0 is even.*

Claim 6. *For some integer k, the integer $8k$ is even.*

Claim 7. *For some integer k, the integer $2k + 3$ is odd.*

Claim 8. *For some integers n and m, the integer $2n + 2m + 1$ is odd.*

Claim 9. *The integer 15 divides the integer 30.*

Claim 10. *For some integer k, $2|(4k + 6)$.*

Hopefully you found the claims in this chapter relatively easy to prove. These basic existence proofs will often appear as a part of larger, more substantive proofs. Later in the semester we will discuss existence proofs that require more than knowledge or arithmetic.