

# Intro to Proofs

Prepared by Mark on March 3, 2025

---

## Part 1:

### Problem 1:

We say an integer  $x$  is *even* if  $x = 2k$  for some  $k \in \mathbb{Z}$ . We say  $x$  is *odd* if  $x = 2k + 1$  for some  $k \in \mathbb{Z}$ . Assume that every integer is even or odd, and never both.

- Show that the product of two odd integers is odd.
- Let  $a, b \in \mathbb{Z}, a \neq 0$ . We say  $a$  *divides*  $b$  and write  $a \mid b$  if there is a  $k \in \mathbb{Z}$  so that  $ak = b$ . Show that  $a \mid b \implies a \mid 2b$
- Show that  $5n^2 + 3n + 7$  is odd for any  $n \in \mathbb{Z}$ .
- Let  $a, b, c$  be integers so that  $a^2 + b^2 = c^2$ . Show that one of  $a, b$  is even.
- Show that every odd integer is the difference of two squares.
- Prove the assumption in the statement of this problem.

**Problem 2:**

Let  $r \in \mathbb{R}$ . We say  $r$  is *rational* if there exist  $p, q \in \mathbb{Z}, q \neq 0$  so that  $r = \frac{p}{q}$

- Show that  $\sqrt{2}$  is irrational.
- Show that the product of two rational numbers must be rational, while the product of irrational numbers may be rational or irrational. If you claim a number is irrational, provide a proof.

**Problem 3:**

Let  $X = \{x \in \mathbb{Z} \mid x \geq 2\}$ . For  $k \geq 2$ , define  $X_k = \{kx \mid x \in X\}$ . What is  $X - (X_2 \cup X_3 \cup X_4 \cup \dots)$ ? Prove your claim.

**Problem 4:**

Show that there are infinitely many primes.

You may use the fact that every integer has a prime factorization.

**Problem 5:**

For a set  $X$ , define its *diagonal* as  $D(X) = \{(x, x) \in X \times X \mid x \in X\}$ .

An *undirected graph*  $G$  is an ordered pair  $(V, E)$ , where  $V$  is a set, and  $E \subset V \times V$  satisfies  $(a, b) \in E \iff (b, a) \in E$  and  $E \cap D(X) = \emptyset$ .

The elements of  $V$  are called *vertices*; the elements of  $E$  are called *edges*.

- Make sense of the conditions on  $E$ .
- The *degree* of a vertex  $a$  is the number of edges connected to that vertex.  
We'll denote this as  $d(a)$ . Write a formal definition of this function using set-builder notation and the definitions above. Recall that  $|X|$  denotes the size of a set  $X$ .
- There are 9 people at a party. Show that they cannot each have 3 friends.  
Friendship is always mutual.

**Problem 6:**

Let  $f$  be a function from a set  $X$  to a set  $Y$ . We say  $f$  is *injective* if  $f(x) = f(y) \implies x = y$ .

We say  $f$  is *surjective* if for all  $y \in Y$  there exists an  $x \in X$  so that  $f(x) = y$ .

Let  $A, B, C$  be sets, and let  $f : A \rightarrow B$ ,  $g : B \rightarrow C$  be functions. Let  $h = g \circ f$ .

- Show that if  $h$  is injective,  $f$  must be injective and  $g$  may not be injective.
- Show that if  $h$  is surjective,  $g$  must be surjective and  $f$  may not be surjective.

**Problem 7:**

Let  $X = \{1, 2, \dots, n\}$  for some  $n \geq 2$ . Let  $k \in \mathbb{Z}$  so that  $1 \leq k \leq n - 1$ .

Let  $E = \{Y \subset X \mid |Y| = k\}$ ,  $E_1 = \{Y \in E \mid 1 \in Y\}$ , and  $E_2 = \{Y \in E \mid 1 \notin Y\}$

- Show that  $\{E_1, E_2\}$  is a partition of  $E$ .  
In other words, show that  $\emptyset \neq E_1$ ,  $\emptyset \neq E_2$ ,  $E_1 \cup E_2 = E$ , and  $E_1 \cap E_2 = \emptyset$ .  
*Hint:* What does this mean in English?
- Compute  $|E_1|$ ,  $|E_2|$ , and  $|E|$ .  
Recall that a set of size  $n$  has  $\binom{n}{k}$  subsets of size  $k$ .
- Conclude that for any  $n$  and  $k$  satisfying the conditions above,

$$\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$$

- For  $t \in \mathbb{N}$ , show that  $\binom{2t}{t}$  is even.

**Theorem 8: The Division Algorithm**

Given two integers  $a, b$ , we can find two integers  $q, r$ , where  $0 \leq r < b$  and  $a = qb + r$ . In other words, we can divide  $a$  by  $b$  to get  $q$  remainder  $r$ .

**Problem 9:**

Let  $x, y \in \mathbb{N}$  be natural numbers. Consider the set  $S = \{ax + by \mid a, b \in \mathbb{Z}, ax + by > 0\}$ .

The well-ordering principle states that every nonempty subset of the natural numbers has a least element.

- Show that  $S$  has a least element. Call it  $d$ .
- Let  $z = \gcd(x, y)$ . Show that  $z$  divides  $d$ .
- Show that  $d$  divides  $x$  and  $d$  divides  $y$ .
- Prove or disprove  $\gcd(x, y) \in S$ .



**Problem 10:**

- Let  $f : X \rightarrow Y$  be an injective function. Show that for any two functions  $g : Z \rightarrow X$  and  $h : Z \rightarrow X$ , if  $f \circ g = f \circ h$  from  $Z$  to  $Y$  then  $g = h$  from  $Z$  to  $X$ .

By definition, functions are equal if they agree on every input in their domain.

*Hint:* This is a one-line proof.

- Let  $f : X \rightarrow Y$  be a surjective function. Show that for any two functions  $g : Y \rightarrow W$  and  $h : Y \rightarrow W$ , if  $g \circ f = h \circ f \implies g = h$ .
- ★ Let  $f : X \rightarrow Y$  be a function where for any set  $Z$  and functions  $g : Z \rightarrow X$  and  $h : Z \rightarrow X$ ,  $f \circ g = f \circ h \implies g = h$ . Show that  $f$  is injective.
- ★ Let  $f : X \rightarrow Y$  be a function where for any set  $W$  and functions  $g : Y \rightarrow W$  and  $h : Y \rightarrow W$ ,  $g \circ f = h \circ f \implies g = h$ . Show  $f$  is surjective.

**Problem 11:**

In this problem we prove the binomial theorem: for  $a, b \in \mathbb{R}$  and  $n \in \mathbb{Z}^+$ , we have

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

In the proof below, we let  $a$  and  $b$  be arbitrary numbers.

- Check that this formula works for  $n = 0$ . Also, check a few small  $n$  to get a sense of what's going on.
- Let  $N \in \mathbb{N}$ . Suppose we know that for a specific value of  $N$ ,

$$(a + b)^N = \sum_{k=0}^N \binom{N}{k} a^k b^{N-k}$$

Now, show that this formula also works for  $N + 1$ .

- Conclude that this formula works for all  $a, b \in \mathbb{R}$  and  $n \in \mathbb{Z}^+$ .

**Problem 12:**

A *relation* on a set  $X$  is an  $R \subset X \times X$ .

- We say  $R$  is *reflexive* if  $(x, x) \in R$  for all  $x \in X$ .
- We say  $R$  is *symmetric* if  $(x, y) \in R \implies (y, x) \in R$ .
- We say  $R$  is *transitive* if  $(x, y) \in R$  and  $(y, z) \in R$  imply  $(x, z) \in R$ .
- We say  $R$  is an *equivalence relation* if it is reflexive, symmetric, and transitive.

Say we have a set  $X$  and an equivalence relation  $R$ .

The *equivalence class* of an element  $x \in X$  is the set  $\{y \in X \mid (x, y) \in R\}$ .

Let  $R$  be an equivalence relation on a set  $X$ .

Show that the set of equivalence classes is a partition of  $X$ .

**Problem 13:**

Show that there exist two positive irrational numbers  $a$  and  $b$  so that  $a^b$  is rational.

**Problem 14:**

Show that the following holds for any planar graph:

$$\text{vertices} - \text{edges} + \text{faces} = 2$$

*Hint:* If you don't know what these words mean, ask an instructor.

**Problem 15:**

Consider a rectangular chocolate bar of arbitrary size.

What is the minimum number of breaks you need to make to separate all its pieces?

**Problem 16:**

Four travellers are on a plane, each moving along a straight line at an arbitrary constant speed.

No two of their paths are parallel, and no three intersect at the same point.

We know that traveller A has met traveler B, C, and D, and that B has met C and D (and A).

Show that C and D must also have met.

**Problem 17:**

Say we have an  $n$ -gon with non-intersecting edges.

What is the size of the smallest set of vertices that can “see” every point inside the polygon?