

# Proof Workshop

February 9, 2024

## Contents

<b>1 Day 3: Induction and Algebraic Thinking</b>	<b>1</b>
1.1 Mathematical Induction . . . . .	1
1.1.1 Exercises . . . . .	3
1.2 The Peano Axioms . . . . .	4
1.3 Thinking about Proofs . . . . .	5
1.3.1 Exercises . . . . .	5

## 1 Day 3: Induction and Algebraic Thinking

### 1.1 Mathematical Induction

The last basic proof technique is **mathematical induction**. It is designed for proving statements about the natural numbers.

Suppose we want to show some property  $P$  is true for all natural numbers  $0, 1, 2, \dots$ . We can't check that all of these numbers individually satisfy the property since there are infinitely many of them. However, what we can show is that if  $n$  satisfies  $P$ , then  $n + 1$  also satisfies  $P$ . Then, if we show that  $0$  satisfies  $P$ , then it follows so does  $0 + 1 = 1$ , and so does  $1 + 1 = 2$ , and so on until all the natural numbers satisfy  $P$ .

Therefore, to prove a statement of the form  $\forall n \in \mathbb{N}, P(n)$ ,

1. Prove  $P(0)$ . This is called the *base case*.
2. Prove that  $\forall n \in \mathbb{N}, P(n) \implies P(n + 1)$ . This is called the *induction step*, and the assumption that  $P(n)$  is true is called the *induction hypothesis*.

We often signify we will use induction by saying "we will proceed by induction on  $n$ " or something similar. It helps to explicitly label "base case" or "induction step."

**Example 1.1.** Prove that for every natural number  $n$ ,  $2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1$ .

We proceed by induction on  $n$ .

Base case: We have  $2^0 = 2^1 - 1 = 1$ .

Induction Step: Suppose  $\sum_{i=0}^n 2^i = 2^{n+1} - 1$ . We will show  $\sum_{i=0}^{n+1} 2^i = 2^{n+2} - 1$ . Adding  $2^{n+1}$  to  $\sum_{i=0}^n 2^i$ , we get

$$\sum_{i=0}^{n+1} 2^i = \sum_{i=0}^n 2^i + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1} = 2(2^{n+1}) - 1 = 2^{n+2} - 1.$$

**Example 1.2.** For every natural number  $n \geq 5$ ,  $2^n > n^2$ .

We proceed by induction on  $n$ .

Base Case: For  $n = 5$ , we have  $2^5 = 32 > 25 = n^2$ .

Induction Step: Let  $n \geq 5$  be arbitrary, and assume  $2^n > n^2$ . Then

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &> 2n^2 \\ &= n^2 + n^2 \\ &\geq n^2 + 5n \text{ since } n \geq 5 \\ &= n^2 + 2n + 3n \\ &> n^2 + 2n + 1 = (n+1)^2 \end{aligned}$$

**Example 1.3.** For every real number  $x > -1$  and every natural number  $n$ ,  $(1+x)^n > nx$ .

Let  $x > -1$  be arbitrary. We will show by induction that  $(1+x)^n \geq 1+nx$ . It clearly follows that  $(1+x)^n > nx$ .

Base case: if  $n = 0$ , then  $(1+x)^n = (1+x)^0 = 1 = 1+nx$ .

Induction step: suppose  $(1+x)^n \geq 1+nx$ . Then

$$\begin{aligned} (1+x)^{n+1} &= (1+x)(1+x)^n \\ &\geq (1+x)(1+nx) \\ &= 1+x+nx+nx^2 \\ &= 1+(n+1)x \end{aligned}$$

since  $nx^2 \geq 0$ .

**Strong Induction.** Sometimes, it's not enough to prove that a natural number has a certain property only assuming the previous one does. We need something stronger, and need to assume *all* smaller natural numbers have this property. This is called *strong induction*.

To prove a statement of the form  $\forall n \in \mathbb{N}, P(n)$ :

Prove that  $\forall \in \mathbb{N}, [(\forall k < n, P(k)) \implies P(n)]$ . This means that we let  $n$  be a natural number, assume  $P(k)$  for all  $k < n$ , and then prove  $P(n)$ .

Note that you don't need to prove a base case for the statement. This is because for  $n = 0$ , there are no  $k < n$ ; so the assumptions are vacuous and we prove  $P(0)$  independently.

The two forms of induction are actually equivalent; see [https://en.wikipedia.org/wiki/Mathematical\\_induction#Complete\\_\(strong\)\\_induction](https://en.wikipedia.org/wiki/Mathematical_induction#Complete_(strong)_induction) for a quick discussion of this. Every proof by ordinary induction can be converted into one by strong induction, and vice versa, so you can't actually prove anything *stronger*; it is just easier.

**Example 1.4.** Every integer  $n > 1$  is either prime or a product of primes.

We will show this by strong induction. Suppose  $n > 1$  and suppose every integer  $1 < k < n$  is either prime or a product of primes. If  $n$  is prime there is nothing to prove, so suppose  $n$  is not prime. By the definition of primeness, this means there are numbers  $a, b < n$  such that  $ab = n$ . Note that since  $a < n = ab$ , it follows  $b > 1$  and similarly  $a > 1$ . Then, by the inductive hypothesis,  $a$  and  $b$  are each either prime or a product of primes. Since  $n = ab$ ,  $n$  is a product of primes.

**1.1.1 Exercises**

1. ★ Show that

$$\sum_{k=1}^n k = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

2. Show that

$$\sum_{k=1}^n k^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

3. ★ Recall the
- binomial coefficients**
- are defined as

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Now assume **Pascal's identity**:

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

Prove the **binomial theorem**: for all integers  $n \geq 0$ ,

$$(x+y)^n = \binom{n}{0}x^n y^0 + \binom{n}{1}x^{n-1}y^1 + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}x^1y^{n-1} = \sum_{k=0}^n \binom{n}{k}x^k y^{n-k}.$$

where these are polynomials in the variables  $x, y$ .

4. Show that  $\sum_{k=1}^n \binom{n}{k} = 2^n$ . (Hint: use induction and Pascal's identity).
5. Show that  $1 + 3 + 5 + 7 + \cdots + (2n-1) = \sum_{k=1}^n (2k-1) = n^2$  (Hint: if you assume problem 1, you don't need induction).
6. Show that  $5^n - 1$  is divisible by 4 for every positive integer  $n$ .
7. ★ Show that 2 divides  $n^2 + n$  for all positive integers  $n$ .
8. Show that for all positive integers,  $n! \leq n^n$ .
9. Show that  $n! > 2^n$  for all integers  $n \geq 4$ .
10. ★ Show that every nonempty subset of  $\mathbb{N}$  has a minimal element.
11. ★ Find the error in the following proof by induction, which asserts that all horses are of the same color.

Our proof will show that for each  $n$ , any group of  $n$  horses must be of the same color. Clearly this implies that all horses are of the same color.

Base case:  $n = 0$ . A group of 0 horses vacuously has the same color, so the base case is satisfied.

Inductive step: assuming all groups of horses of size  $n - 1$  have the same color, take some arbitrary set  $S$  of horses of size  $n$ . Separate the set into two subsets of size  $n - 1$ ,  $S_1$  and  $S_2$ , by removing the first and last horse, respectively. By the inductive step, the horses in  $S_1$  all have the same color, and the same for the horses in  $S_2$ . Since both groups share the same color as the horses in  $S_1 \cap S_2$ , the horses in  $S_1$  and  $S_2$  must have the same color. QED.

## 1.2 The Peano Axioms

We follow the presentation of Terence Tao's *Analysis I*

So far, we have been taking as a given the definitions of the natural numbers  $\mathbb{N}$ , the integers  $\mathbb{Z}$ , the rationals  $\mathbb{Q}$ , the reals  $\mathbb{R}$ , and the various operations  $+$ ,  $\cdot$ ,  $-$ ,  $/$ . But *why* do these rules work at all? What do we really mean when we say that  $2 + 2 = 4$ ? How are addition, multiplication, and exponentiation defined?

The answer is actually quite hard. One problem is that, while we are working with the basic rules, we must not assume the things that we are already familiar with, but have not *proved*. We cannot assume that  $a + b = b + a$ , for example. We will begin by defining the natural numbers (for us, they include 0). From this, we may define addition. Repeated addition gives us multiplication. Then, repeated multiplication gives exponentiation.

What is addition? It is just the repeated process of *incrementing*, or counting forward. Incrementing seems to be the fundamental operation; we learn to count starting from 0, and then adding a number each to count up.

Thus, to define the natural numbers we start with two things: the zero number 0, and the increment operation. We will use  $n++$  to denote the *successor* of  $n$  (some denote it  $\text{succ}(n)$ ).

### Axioms 1.5. The Peano Axioms

1. 0 is a natural number.
2. If  $n$  is a natural number, then  $n++$  is also a natural number.
3. 0 is not the successor of any natural number, i.e. we have  $n++ \neq 0$  for every natural number  $n$
4. Different natural numbers must have different successors, i.e. if  $n, m$  are natural numbers and  $n \neq m$ , then  $n++ \neq m++$ . Equivalently, if  $n++ = m++$  then we must have  $n = m$ .
5. (Principle of mathematical induction) Let  $P(n)$  be any property depending on a natural number  $n$ . Suppose that  $P(0)$  is true, and suppose that whenever  $P(n)$  is true,  $P(n++)$  is also true. Then  $P(n)$  is true for every natural number  $n$ .

Axioms 1 – 5 are called the *Peano axioms* for the natural numbers.

There is an additional axiom, more properly belonging to set theory:

**Axiom 7.** (Infinity).

There exists a set  $\mathbb{N}$ , whose elements are called natural numbers, as well as an object 0 in  $\mathbb{N}$ , and an object  $n++$  assigned to every natural number  $n \in \mathbb{N}$ , such that the Peano axioms hold.

Thus we take it as an axiom of sets that there is an object that satisfies the Peano axioms. Elements of the natural numbers are of the form  $0++$ ,  $(0++)++$ ,  $((0++)++)++$ , etc. As a matter of notation, we define 1 to be the number  $0++$ , 2 to be  $(0++)++$ , and so on.

**Remark 1.** If you are interested in learning more about the foundations of mathematics and formal proofs, we highly recommend the Natural Numbers Game, hosted at [https://www.ma.imperial.ac.uk/~buzzard/xena/natural\\_number\\_game/](https://www.ma.imperial.ac.uk/~buzzard/xena/natural_number_game/). In a game-like environment you will prove many properties of the natural numbers and functions in Lean, a formal theorem proving system.

### 1.3 Thinking about Proofs

We now have a few basic proof techniques under our belts: direct proof, proof by contradiction, proof by counterexample, proof of the contrapositive, and proof by induction. We devote the remainder of today's time to practicing applying these to various statements and discussing how to think about proofs.

**Example 1.6.** Show that  $x \in \mathbb{Z}$  is even  $\iff x^2$  is divisible by 4.

To prove the forward direction, let's assume that  $x$  is even, so  $x = 2k$  for  $k \in \mathbb{Z}$ . Then  $x^2 = (2k)^2 = 4k^2$ , so 4 divides  $x^2$ .

That was easy; it was very straightforward to extract information about  $x^2$  given information about  $x$ . It would be nice if we could prove the other direction in a similar manner.

Luckily, we can, by proving the contrapositive of the other direction; that is, that  $x$  odd  $\implies x^2$  not divisible by 4. We write  $x = 2k + 1$  for  $k \in \mathbb{Z}$ . Then

$$x^2 = (2k + 1)^2 = 4k^2 + 4k + 1.$$

This will clearly have a remainder of 1 when divided by 4, so this is not divisible by 4. This shows that  $x^2$  being divisible by 4 implies that  $x$  is even, so we have shown the if-and-only-if statement.

The moral here is that if proving one direction of an if-and-only-if statement is particularly simple, you may have an easier time proving the contrapositive of the other direction, as such a proof would likely be of a similar nature to the first direction.

**Example 1.7.** Can every  $n \in \mathbb{N}$  be written as the sum of two squares, that is,  $n = a^2 + b^2$  for  $a, b \in \mathbb{Z}$ ? Prove or give a counterexample.

Let's first think of how we would prove that this statement is true. Given an arbitrary natural number  $n$ , we would need to exhibit two integers  $a$  and  $b$ , dependent on  $n$ . Since  $n$  is arbitrary, we have very little information to use to cook up an  $a$  and  $b$ , so this strategy is unlikely to work.

We could perhaps try induction, as this is a statement about all natural numbers. However, even if  $n = a^2 + b^2$ , then all we know is that  $n + 1 = a^2 + b^2 + 1$ , and there is no guarantee that any of  $a^2 + b^2$ ,  $a^2 + 1$ , or  $b^2 + 1$  are squares.

In general, it seems we do not have enough information about any random  $n$  to prove this statement. This suggests that it is not true for all  $n$ , and we may need to know some special properties about  $n$  to show it can be written as a sum of two squares. This tells us to move to finding a counterexample.

Starting simple,  $1 = 1^2 + 0^2$  and  $2 = 1^2 + 1^2$ , so those don't work. However, we can only write 3 as  $1 + 2$  or  $3 + 0$ , and neither 2 nor 3 are squares. This gives a counterexample.

We now open the floor to the types of proofs and problems you would like to practice thinking through.

#### 1.3.1 Exercises

1. ★ Show that  $2 + 2 = 4$ .
2. Show that for all natural numbers  $n$  and  $m$ ,  $n + m = m + n$ . (Hint: induct on  $n$ ).

3. ★ Let  $a, b, c$  be natural numbers such that  $a + b = a + c$ . Show that  $b = c$ .
4. (Harder, skip this on first passing). Prove associativity: For all natural numbers  $a, b, c$ , we have  $(a + b) + c = a + (b + c)$ .
5. Show that  $2 \times 2 \times 3 = 6$ .
6. Let  $m, n$  be natural numbers. Then  $n \times m = m \times n$ .
7. For all natural numbers  $a, b, c$ , show that  $a(b + c) = ab + ac$ .
8. Show that  $2^2 = 4$ .
9. Show that for any natural numbers  $a, b, c$ , we have  $(a \times b) \times c = a \times (b \times c)$ .