The Number Theory Companion

Authors: Ahmed, Jai, and Swayam

Contents

CHAPTER 1

Introduction to rigorous proofing

Number theory, one of the oldest and most active departments of mathematics, is renowned for its theoretical breadth and cross-disciplinary applications to subjects like representation theory, physics, and cryptography. The cutting edge of number theory is full of complex and well-known open issues; at its core, though, are simple, fundamental concepts that may intrigue and test beginning students.

The first thing we did, as humans, was that we observed the relations between things and looked at them more abstractly. The first number we discovered we "one". Then we have discovered "two ones" after long time. Then we came to discover all numbers, but this took us centuries of hard work of many mathematicians.

This companion was designed specially to enrich you with the right way to think about math **rigorously**. It will lead you to discover the beauty of math yourself. Each chapter will improve your numbers sensing abilities that will convince your mind more than any other thing you have seen in your life.

1.1 Mathematical axioms

Mathematical Axioms are the fundamental building blocks of all rigorous math proof. Axioms are presented as self-evident truths on which you may construct any defenses or deductions. These are broad truths that are acknowledged by everybody. All you need to discover the nature of mathematics are these axioms and some imagination. We will lead to prove more complex theories such as the *prime factorization theorem*: *every number can be factorized into primes numbers in one and only one unique way.*

This book is not going to provide you with the way to be the fastest human calculator, but it is more about developing your numerical curiosity and seeing the relations between numbers at a glance.

The arithmetic are based on laws that build up the general and more advanced theories. They can be expressed as follows.

1. *Closure Property*

$$a + b \in \mathbb{Z}$$

$$a - b \in \mathbb{Z}$$

2. *Commutative property*

$$a + b = b + a$$

$$a \times b = b \times a$$

3. *Identity Property*
$$a + 0 = a$$
$$a \times 1 = a$$

4. *Associative property*
$$a + (b + c) = (a + b) + c$$
$$a \times (b \times c) = (a \times b) \times c$$
$$a \times b \in \mathbb{Z}$$

5. *Distributive Property*
$$a \times (b + c) = a \times b + a \times c$$

6. *Well ordering Principle* Every nonempty subset S of the positive integers has a least element.

7. *Cancellation law*: If a, b, and c are integers with $a \times c = b \times c$, $c \neq 0$, then $a = b$.

8. There is a unique element $0 \in \mathbb{Z}$ such that $\forall a \in \mathbb{Z}, 0 + a = a + 0 = a$

9. *additive inverse:* $\forall a \in \mathbb{Z}$, there is a unique element $-a \in \mathbb{Z}$ such that $a+(-a) = (-a)+a = 0$

10. *Trichotomy*: If $a \in \mathbb{Z}$, then is has one of the following three states
$$a = 0,$$
$$a > 0,$$
$$a < 0$$

We are going to mention these axioms along this book to build your rigorous understanding of math. You may think of that any number multiplied by zero is zero for granted, but it is actually can be proven using the previous axioms.

Problem 1.1.1. Proof that $0 \times a = 0$ $\forall a$. True in $\mathbb{Z}$.

Proof.

$$\begin{aligned}
0 \times a &= (0 + 0) \times a, && \text{(additive identity)}\\
0 \times a &= 0 \times a + 0 \times a, && \text{(Distributive property)}\\
0 \times a + (-0 \times a) &= (0 \times a + 0 \times a) + (-0 \times a), && \text{(additive inverse)}\\
(0 \times a + (-0 \times a)) &= 0 \times a + (0 \times a + (-0 \times a)), && \text{(Associativity)}\\
0 &= 0 \times a + 0, && \text{(additive inverse)}\\
0 &= 0 \times a && \text{(additive identity)}
\end{aligned}$$

■

Here are a couple of more examples about the rigorous proofing methods.

Problem 1.1.2. $a < b$ and $b < c \Rightarrow a < c$.

Proof. We have if $a < b \Rightarrow b = a + k$, and $b < c \Rightarrow c = b + m$ for some $k, m \in \mathbb{N}$.
By substituting,

$$\begin{aligned} c &= (a + k) + m, && \text{(Associativity)} \\ c &= a + (k + m), && \text{(Associativity)} \\ c &> a, && \text{(definition of inequality)} \\ a &< c \end{aligned}$$

■

Problem 1.1.3. $a < b$ and $c > 0 \Rightarrow ac < bc$. True in $\mathbb{Z}$.

Proof. We have if $a < b \Rightarrow b = a + k$, for some $k \in \mathbb{N}$).
By multiplying both sides by c,

$$\begin{aligned} bc &= (a + k)c, && \text{(closure property)} \\ bc &= (ac) + (kc), && \text{(Distributive property)} \\ bc &= ac + (kc), && \text{(Associative property)} \\ bc &> acc, && \text{(Definition of inequality)} \end{aligned}$$

Since we have k and $c \in \mathbb{N}$, $(kc) \in \mathbb{N}$ by (closure property). ■

It is now your turn to do some problems. You have to try these problems yourself and you can find hints at the end of this book.

Problem 1.1.4. There are no integers strictly between 0 and 1.(Hint: Use well-ordering principle)

Problem 1.1.5. Every non-empty subset of $\mathbb{Z}$ which is bounded above has a largest element. (Hint: Use well-ordering principle)

1.2 Mathematical Induction

The basic idea behind induction is hidden in the following gem: prove the statement for some $n = a$. Then, prove that if the statement holds for $n = k$, then it must hold for $n = k + 1$. Therefore, since the statement holds for $n = a$, it must hold for $n = a + 1$,$a + 2$,$a + 3$, and so on. This is why induction is typically used when we wish to prove a statement for all integers.

Theorem 1.2.1 (Principle of Induction)**.** *To show a statement is true for* ***all positive integers****, we can do it through induction by the following steps:*

- *Show it is true for some starting values (known as the* ***base case****), most likely $n = 0$ or $n = 1$.*
- *Then, we show that if it is true for $n = k$, the statement is true for $n = k + 1$.*

So why does this work? We can imagine a sequence of dominoes[1]:

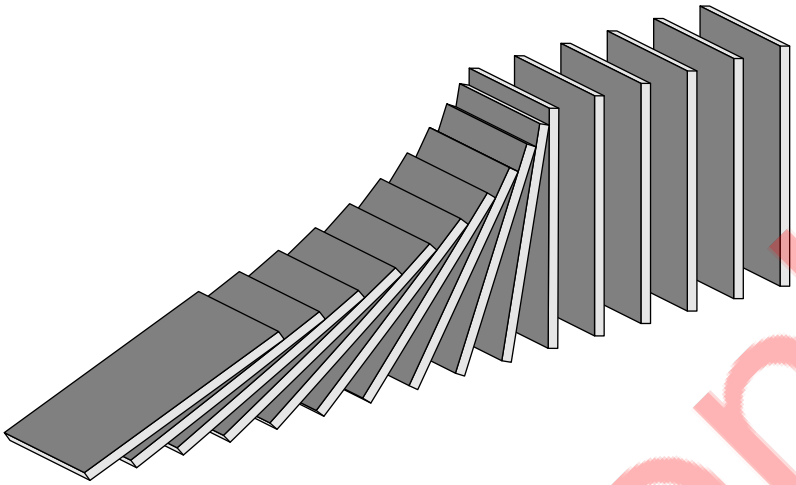

Figure 1.1: A row of dominoes, falling and knocking the next one over, the process repeating infinitely.

We can use this figure to explain induction. Imagine the first domino is our base case $n = 0$ (a similar argument can be repeated for other starting values such as $n = 1$). We show that it is true, so we knock that domino over. Then, this knocks the next domino over ($n = 1$), which knocks the next domino over ($n = 2$), and the process continues infinitely. Let's see an example:

Conjecture 1.2.1 (Faulhaber)**.** *Show that the sum*

$$1 + 2 + \cdots + n$$

has value equal to

$$\frac{n(n+1)}{2},$$

where n is any positive integer.

Remark 1.2.1. In induction, we are often given formulas and asked to prove them. How we got those formulas is another story called derivation.

Proof. We are given the formula $\frac{n(n+1)}{2}$ and are trying to prove this for all positive integers starting with 1, then $2, 3, 4$, and so on. We shall use our induction (or domino principle, whichever you fancy) to show this. We first need to show the statement is true for our base case.

Base Case 1. *We start by proving the base case of $n = 1$ because 1 is the smallest positive integer. This is a fairly simple sum because the sum of the first integer is simply 1. We can verify that the given formula holds by plugging 1 for n. We get*

$$\frac{1(1+1)}{2} = \frac{1 \cdot 2}{2} = \frac{2}{2} = 1.$$

Now we know that the given formula works for $n = 1$.

[1] Credits to Amol Rama for this image.

Now we can perform our two induction steps.

Inductive Hypothesis 1. *Inductive Hypothesis Assume that the formula* $\frac{n(n+1)}{2}$ *calculates the sum of the first* k *positive integers when* $n = k$.

Now, we finish off with the last part, which is the inductive step.

Inductive Step 1. *Inductive Step Assume that the given formula holds for* $n = k$ *for some* k. *Then we must prove that it also holds for* $n = k + 1$. *Let us now try to calculate*

$$1 + 2 + 3 + \cdots + k + (k + 1)$$

Because of the Inductive Hypothesis, we know that we can use our formula to calculate the value of

$$1 + 2 + 3 + \cdots + k$$

by computing $\frac{k(k+1)}{2}$. *We can replace the* $1 + 2 + 3 + \cdots + k$ *part of our sum with this. Then,*

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

Factoring out $k + 1$ *from the right side, we get* $(k + 1)\left(\frac{k}{2} + 1\right)$. *Writing the term* $\frac{k}{2} + 1$ *as a single fraction with 2 as the denominator, this term becomes*

$$\frac{k}{2} + 1 = \frac{k}{2} + \frac{2}{2} = \frac{k + 2}{2}$$

Substituting this last expression for $\frac{k}{2} + 1$ *in* $(k + 1)\left(\frac{k}{2} + 1\right)$, *we have* $(k + 1) \cdot \frac{(k+2)}{2}$ *or* $\frac{(k+1)(k+2)}{2}$. *This cannot be simplified further, so we confirm that when* $k + 1$ *is substituted into our formula, the same result is yielded. Indeed, substituting* n *with* $k + 1$ *in our formula, we get*

$$\frac{(k + 1)(k + 1 + 1)}{2} = \frac{(k + 1)(k + 2)}{2}.$$

These two are the same! Therefore, we can conclude that if our formula works for $n = k$, *then it must work for* $n = k + 1$. *Remember that we established that this formula works for* $n = 1$ *in our base case. Now that we know that it works for* $n = 1$, *we can use our recently proven conclusion to find that the formula works for* $n = 1 + 1 = 2$, *so* $n = 1$ *implies* $n = 2$. *Similarly, our formula works for* $n = 3, 4, 5, \ldots$, *and therefore, we have proven this formula for all positive integers* n.

■

Problem 1.2.1. Try to show that the sum of the first n odd integers is n^2 by the Principle of Induction.

Problem 1.2.2. Try to show that the sum

$$1^2 + 2^2 + 3^2 + \cdots + n^2$$

is equal to

$$\frac{n(n + 1)(2n + 1)}{6}$$

by the Principle of Induction.

Remark 1.2.2 (The Fibonacci Numbers). For the next few exercises, you will work with the Fibonacci numbers. We denote the nth Fibonacci number as F_n. We define $F_0 = 0$ and $F_1 = 1$. Then, for $n \geq 2$,

$$F_n = F_{n-1} + F_{n-2}.$$

Therefore, $F_2 = F_1 + F_0 = 1 + 0 = 1$, $F_3 = F_2 + F_1 = 1 + 1 = 2$, $F_4 = F_3 + F_2 = 2 + 1 = 3$, and so on. Here are the first few Fibonacci numbers:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \cdots$$

(Can you list out a couple more?) It turns out that the Fibonacci numbers have very interesting properties.

Problem 1.2.3. Prove that for $n \geq 1$,

$$F_{n-1}F_{n+1} = F_n^2 + (-1)^n$$

using the Principle of Induction.

Problem 1.2.4. Prove that

$$F_n = F_{n-2} + F_{n-3} + F_{n-4} + \cdots + F_1 + F_0 + 1$$

using the Principle of Induction.

Problem 1.2.5. Prove that

$$F_0^2 + F_1^2 + F_2^2 + F_3^2 + \cdots + F_n^2 = F_n F_{n+1}$$

using the Principle of Induction.

1.3 Pigeonhole Principle

This next theorem is not a proofs strategy, but merely a concept. This concept is so trivial that no one thought it to be significant for a long time. In this concept, we assume that we have pigeons that live in holes. We put these pigeons into their holes by choosing one hole for each pigeon. This is the same as putting toy balls into different buckets, where the pigeons are the balls and the holes are the buckets.

Conjecture 1.3.1 (Pigeonhole Principle)**.** *If we have $n + 1$ pigeons and only n holes to place them in, we must have at least 2 pigeons in one of the holes.*

Proof. The proof for this observation is simple. We can use the method of Proof by Contradiction. We assume that we can place the pigeons into their holes such that there is no more than one pigeon per hole. Suppose we are now placing our pigeons into their holes. If we place more than one pigeon per hole, we have at least 2 pigeons per hole. Therefore, we must place one pigeon per hole. By the time we have place a single pigeon in each of the n holes, we have one pigeon remaining. No matter where we place this pigeon, it will end up in a hole with two pigeons in it. Therefore, it is unavoidable to have at least two pigeons in one of the pigeonholes. ■

This conjecture is so trivial, you probably did not need to read the proof in order to assure yourself that it was true. The next conjecture that we prove is a generalization of this previous one.

Conjecture 1.3.2 (Generalized Pigeonhole Principle)**.** *If we have $n \cdot k + 1$ pigeons and must place them into n different holes, we must have at least $k + 1$ pigeons in one of the n holes.*

Proof. We do this proof by the method of Proof by Contradiction as well. Suppose that all of the holes have less than $k + 1$ pigeons. We can therefore place up to k pigeons per hole. Armed with a strategy, we start to confidently place k pigeons in each hole. However, when we reach the last hole and place the k pigeons, we realize that we have only used

$$n \text{ holes} \times k \text{ pigeons per hole} = n \cdot k \text{ pigeons},$$

and that we still have one pigeon left to place in one of the holes (because we started with $n \cdot k + 1$ pigeons). Similar to the last proof, no matter where we place our last pigeon, it will end up in a hole which has $k + 1$ pigeons in it (because we had originally put k pigeons in every hole). Therefore, it is unavoidable to have $k + 1$ pigeons in one of the n holes. ■

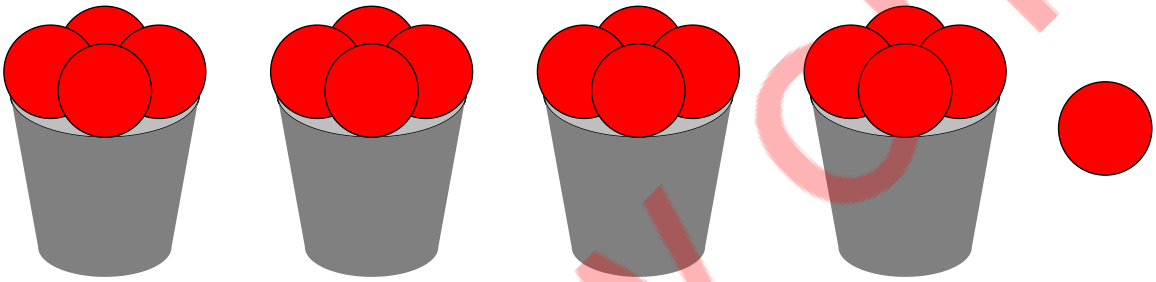

Figure 1.2: This diagram shows this principle visually if we have $4 \cdot 4 + 1 = 17$ balls. By placing 4 balls in each of the 4 buckets, we use 4 buckets $\times$ 4 balls per bucket $= 16$ balls. However, we have one ball remaining. This ball must be kept in a bucket which will end up having $4 + 1 = 5$ balls.

Remark 1.3.1. In the image above[2], we used the analogy of balls and buckets. Note that this is exactly the same as using pigeons and pigeonholes, respectively. There are many analogies for the pigeonhole principle, but you will start to recognize them with enough practice.

This generalization is fairly harder to grasp, but it still comes intuitively to the mind. While this generalization has applications of its own (such as in basic competition math problems), it can also be used to prove more advanced theorems. Let us simply establish our results for now:

Theorem 1.3.1 (Pigeonhole Principle)**.** *If we have at least $n \cdot k + 1$ pigeons and must place them into n different holes, we must have at least $k + 1$ pigeons in one of the n holes.*

Problem 1.3.1 (Art of Problem Solving)**.** Use the Pigeonhole Principle to attempt the following problem: If a Martian has an infinite number of red, blue, yellow, and black socks in a drawer, how many socks must the Martian pull out of the drawer to guarantee he has a pair?

Problem 1.3.2 (Art of Problem Solving)**.** Prove that if we select 5 points within the boundaries of a unit square, then some pair of them are no more than $\sqrt{2}/2$ apart. (Hint: Divide the square into 4 parts to use the Pigeonhole Principle.)

[2] Credits to Amol Rama for this image.

1.4 Infinite Descent

A proof by infinite descent, also referred to as Fermat's method of descent, is a specific type of proof by contradiction used to demonstrate that a statement cannot possibly hold for any number. It does this by demonstrating that if the statement were to hold for a number, it would also be true for a smaller number, resulting in an infinite descent and ultimately a contradiction. This technique, which is based on the well-ordering principle, is often used to demonstrate that some equations have no solutions such as a specific equations of Diophantine equation.

This specific type of proofing method was widely used after Fermat's proof for the sum of two squares theorem: *an odd prime p can be expressed as a sum of two squares if and only if it is 1(mod 4).* This "1(mod 4)" refers to being one more a multiple of 4, which will be explained later in this book.

The general idea is to show if an equation has an integer nonnegative solution, then it forces the existence of smaller solutions: $a_1 > a_2 > a_3 > \cdots > 0$, which can't be true in $\mathbb{Z}^+$. Since the purpose of this book is to introduce you to the rigorous proofing, this is the rigorous definition of *Infinite Descent.*

Theorem 1.4.1. *Let F be a function that defines a property for non-negative integers such that*

$$F(n)\text{:}"n \text{ satisfies property } F."$$

This following sequence is used to prove $F(n)$ is false for large enough n.

Suppose $k \in \mathbb{Z}^+ \cup \{0\}$.

- *$F(k)$ is not true;*
- *if $F(m)$ is true for a positive integer $m > k$, then there is some smaller i, $m > i \geq k$, for which $F(i)$ is true.*

Then $F(n)$ is false $\forall n \geq k$.

Example 1.4.1. Proof that $\sqrt{2}$ is irrational.

Proof. Suppose to the contrary that $\sqrt{2} \in \mathbb{Q}$, then there exists $a, b \in \mathbb{Z}$ and $(a, b) = 1$ such that $\frac{a}{b} = \sqrt{2}$. By multiplying both sides by b and squaring both sides, we will get $a^2 = 2b^2$. Note that a^2 is even, so $a = 2a'$. By substituting and cancelling, $b^2 = 2a'^2$. By following a similar argument b^2 is even. So, $b = 2b'$, which leads to concluding that $(a, b) > 1$, which contradicts our original assumption. ■

Here is a more beautiful proof using infinite descent.

Proof. Suppose $\sqrt{2} \in \mathbb{Q}$. Note that $1 < \sqrt{2} < 2$. We can say $\sqrt{2} = 1 + \frac{a}{b}$ where a and $b \in \mathbb{Z}$ and $a < b$. By multiplying both sides by b and squaring both sides, we will get $2b^2 = b^2 + 2ab + a^2$. $a^2 = b^2 - 2ab = b(b - 2a)$ leads to saying that $\frac{a}{b} = \frac{b-2a}{a}$. Note that the previous equation has a smaller denominator, so by infinite descent this denominator will hit 1 which leads to a contradiction. ■

Here are some More problems that you can try:

Problem 1.4.1. Find all prime p for which there exist positive integers x, y, and n such that $p^n = x^3 + y^3$. (2000 Hungarian Mathematical Olympiad)