The Number Theory Companion

Authors: Ahmed Metwally, Jai Sharmas, and Swayam Chaulagain

This page intentionally left blank.

Abstract

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. Then 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]:

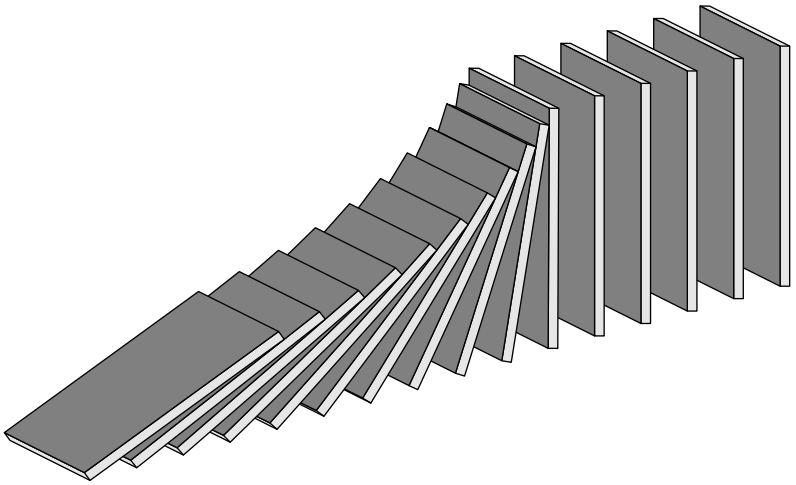

Figure 1.1: A row of dominoes, falling and knocking the next one over, the process repeating infinitely.

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 Mathematical 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 Mathematical 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 Mathematical 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 Mathematical Induction.

Problem 1.2.5. *Prove that*

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

using the Mathematical 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. ■

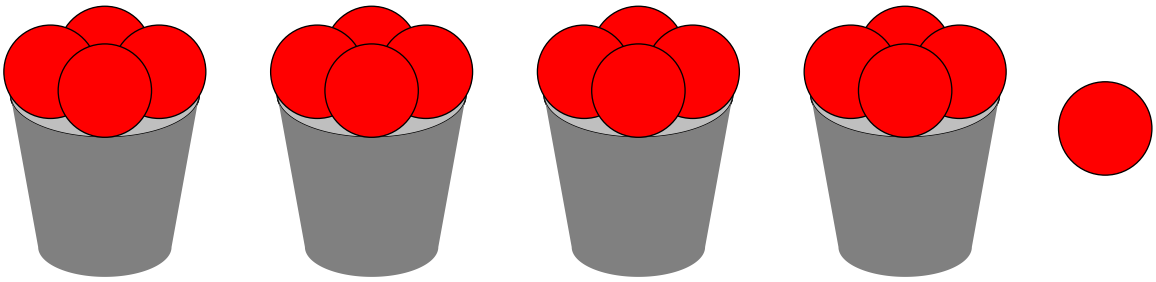

Figure 1.2: This diagram shows this principle visually if we have $4 \cdot 4 + 1 = 17$ balls. By placing 4 balls in each of the 4 buckets, we use 4 buckets $\times$ 4 balls per bucket $= 16$ balls. However, we have one ball remaining. This ball must be kept in a bucket which will end up having $4 + 1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

1.5 Principle of Inclusion-Exclusion

Introduction:

The Principle of Inclusion-Exclusion often called PIE is one of the elementary theories widely used in combinatorics which starts from the Set Theory itself. It is one of the standard methods of counting the total number of elements in the union of any number of finite sets excluding the common element between them.

Recall:

Consider two sets: $A_1 = \{a, b\}$ and $A_2 = \{b, c\}$. Then, $A_1 \cup A_2 = \{a, b, c\}$,and
$|A_1 \cup A_2| = 3$, where $|A_1 \cup A_2|$ equals total number of elements in the union of set A_1 and A_2 .

Thus, we can generalize, If A_1 and A_2 are finite sets, then
$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$. Also, If $A_1, A_2, and A_3$ are finite sets, then
$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_3 \cap A_1| + |A_1 \cap A_2 \cap A_3|$ which is same as,
$|A_1 \cup A_2 \cup A_3| = \sum_{1 \le i \le 3} |A_i| - \sum_{1 \le i < j \le 3} |A_i \cap A_j| + \sum_{1 \le i < j < k \le 3} |A_i \cap A_j \cap A_k|$

Generalization of PIE:

If $A_1, A_2, ..., A_n$ are finite sets, then

$$|A_1 \cup A_2 \cup ..A_n| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| .... + (-1)^{n+1} |A_1 \cap A_2 ..... \cap A_n|$$

Proof By Induction : We need to prove that there is no repetition of any elements and every element is counted only once. Call an element 'a' in n sets. Clearly, WLOG sets having 'a' are $A_1, A_2, .., A_n$.
BaseCase : For $n = 1$, it's trivial that it is counted only once.
Inductivecase : Assuming that this is true for some integer n, then we have to show that it also holds true for $n + 1$.

Let $P = A_1 \cup A_2 \cup ..A_n$. Then, $|A_1 \cup A_2 \cup ..A_n \cup A_{n+1}| = |P \cup A_{n+1}|$
$= |P| + |A_{n+1}| - |P \cap A_{n+1}|$ (1)

Since statement is true for n, $|P| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| .... + (-1)^{n+1} |A_1 \cap A_2 ..... \cap A_n|$. Also,
$|P \cap A_{n+1}| = \sum_{i=1}^{n} |A_i \cap A_{n+1}| - ... + (-1)^{n+1} |(A_1 \cap A_{n+1} \cap ... \cap (A_n \cap A_{n+1})|$
$= \sum_{i=1}^{n} |A_i \cap A_{n+1}| - ... + (-1)^{n+1} |A_1 \cap ... \cap A_n \cap A_{n+1}|$

Substituting all these in (1), we get

$|A_1 \cup A_2 \cup ..A_n \cup A_{n+1}| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| .... + (-1)^{n+1} |A_1 \cap A_2 ..... \cap A_n| + |A_{n+1}| - \sum_{i=1}^{n} |A_i \cap A_{n+1}| + ... + (-1)^{n+2} |A_1 \cap ... \cap A_n \cap A_{n+1}|$

Rearranging them we get,

$|A_1 \cup A_2 \cup ..A_n \cup A_{n+1}| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| ..... + (-1)^{n+2} |A_1 \cap ... \cap A_n \cap A_{n+1}|$.
Thus, true for $n + 1$. QED

Applications:

Pie has got wide range of applications in mathematics starting from set theory itself. It is widely used in counting derangements, counting intersections, total number of onto function,finding permutations in combinatorics and so on. In this section we will take a look at its two main applications.

Counting Intersections:

PIE can be used to count the cardinality of intersection of sets. But using only PIE is not enough, we also need to know De Morgan's law.

De Morgan's Law: $\overline{A_1 \cap A_2 \cap ... \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup ... \cup \overline{A_n}$

Now, Let $\overline{A_n}$ represent the complement of A_n with respect to some universal set A such that $A_n \subset A$ for all values of n.
Then we have.

$$\cap_{i=1}^{n} A_i = \overline{\cup_{i=1}^{n} \overline{A_i}}$$

Thus, we can use the union of set to find it's intersections, which break down the complex problems.

Derangements:

Derangements deals with permutation of objects such that none of the objects is at its previous position. Let's have a look at generalized formula of number of derangements of 'n' objects.

Let A_i be the set of all permutations such that i^{th} position is preserved. We know that $|A_1 \cup A_2 \cup ..A_n|$ is just as same as saying that all the elements will have at least one of the position preserved. Thus we can say derangements is total number of permutations $(n!)$ excluding $|A_1 \cup A_2 \cup ..A_n|$.

$$Derangements(D_n) = n! - |A_1 \cup A_2 \cup ..A_n|$$

Now, using the formula of PIE we get,
$= n! - |A_1 \cup A_2 \cup ..A_n|$
$= n! - [\sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| .... + (-1)^{n+1} |A_1 \cap A_2 ..... \cap A_n|]$

Now we can see clealy that $\sum_{1 \le i \le n} |A_i|$, it is same as $\binom{n}{1}(n-1)!$. Since we are choosing 1 element 'i' from n elements it is $\binom{n}{1}$ and number of elements A_i is $(n-1)!$. Similarly $\sum_{1 \le i < j \le n} |A_i \cap A_j|$ is same as $\binom{n}{2}(n-2)!$. This turns the original equation to

$D_n = n! - [n(n-1)! - \frac{n!}{2!(n-2)!}(n-2)! + ...(-1)^{n+2}\binom{n}{n}(n-n)!]$
$D_n = n!(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + ...(-1)^{n+1}\frac{1}{n!})$. This gives us the generalized formula for derangement that is:

$$\frac{D_n}{n!} = (1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + ...(-1)^{n+1}\frac{1}{n!})$$

Basic Examples:

Example 1:

Each student in Boston College has a subject requirement to graduate from college. It has a economics requirement A and mathematics requirement B. A poll of 130 students shows that: 65 completed A, 40 completed B, 25 completed both A and B. Find the number of students who completed:
(a) At least one of A and B. (b) neither A nor B.

Sol: Given, $|A| = 65, |B| = 40, |A \cap B| = 25, |U| = 130$

(a) $|A \cup B| = |A| + |B| - |A \cap B| = 65 + 40 - 25 = 80$

(b)$|\overline{A \cap B}| = |\overline{A \cup B}| = |U| - |A \cup B| = 130 - 80 = 50$

Example 2:

Four people A,B,C,D,E attend a party leaving their jackets in changing room. After the party, jackets got swapped and was returned to each person in a random manner. Find the probability that none of them get his own jacket using PIE.

Sol: Required Probability $= \frac{Numberofpermutationsinwhichnonegethisjacket}{Totalnumberofpossiblepermutationsofjackets}$

Using the Derangement formula we get,

$= \frac{D_4}{4!}$

$= 4! \frac{[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!}]}{4!}$

$= 1 - 1 + \frac{1}{2} - \frac{1}{6} + \frac{1}{24}$

$= \frac{3}{8}$

PART I

The First Part

CHAPTER 2

Divisibility and modular arithmetic

2.1 Prime Numbers

Primes in the Integers

In our next section, we discuss (arguably) some of the most important numbers: prime numbers. Note that we will start this section by discussing prime numbers in $\mathbb{Z}$ before continuing to other fields. We start off with a definition: A positive integer $n \geq 2$ is prime if and only if it is divisible by 1 and n and none of

$$2, 3, 4, \ldots, n-1.$$

A positive integer that is not prime is referred to as composite.

Remark 2.1.1. Note that this definition of prime numbers is specific to $\mathbb{Z}$. We will see how this generalizes later in the section.

Remark 2.1.2. Note that any positive integer n that is composite can be written as $n = a \cdot b$, where a and b are both greater than 1.

Remark 2.1.3. The number 1 is neither prime nor composite. It is special because it is the product of no primes at all! In other words, if we do not multiply any prime numbers together (or any numbers for that matter), we will end up with the number 1.

Why are prime numbers so important? As we will now see, prime numbers are the building blocks of all numbers.

Conjecture 2.1.1 (Fundamental Theorem of Arithmetic)**.** *Every positive integer greater than* 1 *has a unique way in which it can be written as the product of multiple prime numbers. Specifically, a number n can be written as the product*

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$$

where $p_1, p_2, \ldots, p_m$ are primes and $k_1, k_2, \ldots, k_m$ are positive integers (also known as whole numbers).

Proof. In order to prove this conjecture, we must prove two things:

- Every number has a prime factorization;
- Every number has a unique prime factorization.

Notice how these two parts are in the original conjecture, but we isolated them explicitly. This is a powerful problem solving tool. We perform the following proof for the first part of the conjecture by strong induction, which will be introduced here. Strong induction works similar to normal induction and is founded on the following key ideas:

- Prove a conjecture for some number $n = a$. This is our **Base Case.**
- Prove that if the conjecture is true for

  $$n = a, a + 1, a + 2 \cdots , k - 1,$$

  where $a < k$ (assuming that this is true is known as the **Inductive Hypothesis**), then it must be true for k.
- This last part is the **Inductive Step**. If the conjecture, as proved in the base case, holds for $n = a$, then it must hold for $n = a + 1, a + 2, a + 3, \ldots$, therefore proving the conjecture for $n = k$ for all integers $k \geq a$.

Now, let's get back to proving the Primes in the Integers. We do so with strong induction: Base Case Since 1 is neither prime nor composite, we start with our base case of $n = 2$. Since 2 is prime, we can simply write its prime factorization as 2, and we are done with our base case. Now we proceed to making the: Induction Hypothesis We must assume that all the numbers

$$2, 3, 4, \ldots , k - 1$$

have a prime factorization. Now, we try to find whether k has a prime factorization. This last part is done in the Induction Step k is either prime or composite. If k is prime, then its prime factorization is simply k. However, if k is composite, then we can write k as $k = x \cdot y$, where x and y are positive integers greater than 1 and are either prime or composite (see remark above). Clearly, x and y must be less than k. By our inductive hypothesis, both x and y must both have prime factorizations. Suppose

$$x = p_1^{j_1} \cdot p_2^{j_2} \cdot p_3^{j_3} \cdots p_m^{j_m}$$

and

$$y = q_1^{i_1} \cdot q_2^{i_2} \cdot q_3^{i_3} \cdots q_l^{i_l}.$$

Multiplying these two, we get

$$k = x \cdot y = p_1^{j_1} \cdot p_2^{j_2} \cdot p_3^{j_3} \cdots p_m^{j_m} \cdot q_1^{i_1} \cdot q_2^{i_2} \cdot q_3^{i_3} \cdots q_l^{i_l}.$$

The simplified version of this is the prime factorization of k. Therefore, all numbers $k \geq 2$ have a prime factorization.

Now, we must prove that every number k has a **unique** prime factorization. We can do this using **??**. Suppose that a number n has two prime factorizations so that

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_k$$

and

$$n = q_1 \cdot q_2 \cdot q_3 \cdots q_l$$

where p_i and q_j are distinct primes for all i and j. We need the following

Lemma 2.1.1 (Euclid)**.** *Every prime number $p \mid ab$ (this means p divides the product of a and b) satisfies $p \mid a$ or $p \mid b$.*

We suppose that in the representations of n, we suppose that one of the p_i's is not any of the q_j's. Then, we have that

$$p_i \mid n = q_1^{i_1} \cdot q_2^{i_2} \cdot q_3^{i_3} \cdots q_l^{i_l},$$

so p_i divides one of the q_j, a contradiction. Thus, the two primes are the same. We are only concerned about the exponents now. Let $p_m = q_n$ for some m and n and that these are raised to the powers j_m and i_m, respectively. Assume that for contradiction, $i_m < j_m$ (if not, then we can reverse the roles of the two). Then, considering the number

$$\frac{n}{q_n^{i_n}},$$

we see that two prime factorizations are

$$p_1^{j_1} \cdots p_{m-1}^{j_{m-1}} p_m^{j_m - i_n} p_{m+1}^{j_{m+1}} \cdots p_k^{j_k} = q_1^{i_1} \cdots q_{n-1}^{i_{n-1}} q_{n+1}^{i_{n+1}} \cdots q_l^{i_l}.$$

Notice how there is no $q_n^{i_n}$ on the right hand side because we divided by it. This leads to a contradiction as p_m appears on the left hand side and not on the right hand side (because no other q_x is divisible by p_m). Thus, our original assumption that n has 2 prime factorizations was false, so we know that every positive number greater than one must have a unique prime factorization. ■

Let us establish our new proof technique:

Theorem 2.1.1. *Strong induction is a proofs strategy that works similar to induction. There are 3 parts to a strong induction proof:*

- *Prove a conjecture for some number $n = a$. This is our* ***Base Case.***
- *Assume that the conjecture holds for*

  $$n = a, a+1, a+2 \cdots, k-1,$$

  where $a < k$. This is called the ***Inductive Hypothesis****.*
- *Prove that this conjecture must also hold for k. This last part is the* ***Inductive Step****.*

If the conjecture, as proved in the base case, holds for $n = a$, then it must hold for $n = a+1, a+2, a+3, \ldots$, therefore proving the conjecture for $n = k$ for all integers $k \geq a$.

Because of Primes in the Integers, we can define the following: Every positive integer n greater that 1 can be expressed in the form

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$$

and this is called the **prime factorization** of n. Try your hands at the following exercises: Write the prime factorization of the following numbers: 24, 35, 360. What about 5,040? See the definition of a prime factorization for the writing structure (above). Find the prime factorization of 10. What about 100? 1,000? Try 1,000,000. What about 10^n for some integer n?

Conjecture 2.1.2 (Infinitude of Primes)**.** *There are an infinite number of primes.*

Proof. We can perform this simple proof using **??**. Assume that there is only a finite number of primes $p_1, p_2, p_3, \cdots, p_n$. Now, if we multiply all of these primes together and add one, we get

$$p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1.$$

Let us now find the prime factorization of this number. Uh-oh, we find that our number is not divisible by $p_1, p_2, p_3, \cdots, p_n$. If our new number is prime, then we have found another prime that is not on our finite list of all the primes and therefore we have reached a contradiction. On the other hand, if our number is composite, then it must be divisible by some prime number because it must have a prime factorization. However, it is not divisible by any of the prime numbers in this finite list (it leaves a remainder of when when divided by each of $p_1, p_2, p_3, \cdots, p_n$. In either scenario (whether our number is prime or composite), we have reached a contradiction. Therefore, our original assumption that there is a finite number of primes must have been false. Because of our contradiction, we know that there must be an infinite number of prime numbers. ■

From this proof, we conclude that

Theorem 2.1.2 (Infinitude of Primes)**.** *There are an infinite number of prime numbers.*

Chain of Reasoning

Before extending primes to more fields, it is important to establish a general Chain of Reasoning which shows that if a field has a division algorithm, then it also has unique prime factorization. We will define these terms as we go about this proof.

We start with a definition of primes in general fields:

Examples and Non-Examples of Fields with Unique Prime Factorization

2.2 Quadratic residues

A quadratic residue modulo n is an integer q if and only if it is congruent to a perfect square modulo n, that is, if there is an integer x such that:

$$x^2 = q(\text{mod } n)$$

If the previous equation has no solutions q is called quadratic nonresidue. Quadratic residues are today employed in applications ranging from acoustical engineering to cryptography and the factoring of big numbers. Originally, quadratic residues were an abstract mathematical term from the area of number theory known as modular arithmetic. We can check whether a number is a quadratic residue modulo n or not bi squaring up to $\frac{n}{2} + 1$ (if n is even) or $\frac{n+1}{2}$ (if n is odd). This is due to the fact that $x^2 = (n - x)^2(\text{mod } n)$. The following example shows the quadratic residues modulo 11.

Example 2.2.1.

x	1	2	3	4	5	6	7	8	9	10
x^2	1	4	9	5	3	3	5	9	4	1

We say that 1, 3, 4, 5, and 9 are quadratic residues modulo 11.

Notation

To express if a number is modulo n or not, mathematicians use Legendre symbol to express the quadratic character. Legendre Symbol helps us to determine whether an integer is a quadratic

residue of a prime number using some of its properties. In simple words we can call it as a notation to quadratic residues. In this chapter, we will learn some of the properties of Legendre Symbol, prove some of theorems related to it.

Definition 2.2.1. Let p be an odd prime number and a be an integer such that $p \nmid a$. Legendre symbol $(\frac{a}{p})$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic non residue mod } p \end{cases}$$

Let's look at the example below that will clarify us how this symbol work.

Example 2.2.2. Check if 1, 2, 3, 4 are Q.R. modulo 5.

Taking modulo 5 of squares of these numbers
$1^2 = 1$, $2^2 = 4$, $3^2 = 4$, $4^2 = 1$
Thus,

$$\left(\frac{1}{5}\right) = 1, \left(\frac{2}{5}\right) = -1, \left(\frac{3}{5}\right) = -1, \left(\frac{4}{5}\right) = 1,$$

which means 1,4 are Q.R mod 5 and 2,3 are Q.N.R mod 5.

Euler's Criterion

Now, to understand and prove some of the properties of Legendre Symbol we have to know one of the most important theorem in Number Theory known as Euler's Criterion.

Definition 2.2.2. Let p be an odd prime number and a be an integer. Euler's Criterion $(\frac{a}{p})$ is defined by

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{\text{p}}$$

Proof. We will prove this theorem by breaking them into two cases, since $(\frac{a}{p})$ has got two values:

Case 1: When $(\frac{a}{p}) = 1$. From definition of Legendre Symbol, this means, $x^2 = a(\text{mod p})$. Multiplying both sides by the exponent $\frac{p-1}{2}$ we get, $(x^2)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}(\text{mod p})$.
Now, $a^{\frac{p-1}{2}} = x^{p-1} = 1$ [From Fermat's little Theorem]
Thus, $(\frac{a}{p}) = a^{\frac{p-1}{2}}$.

Case 2: When $(\frac{a}{p})$ = -1. So for $1 \leq k \leq (p-1)$, $kx \equiv a \pmod{\text{p}}$ has a unique solution where $x_0 \not\equiv k$. This one is the most important step in the proof. 1,2,$\cdots$,$(p-$

1)*canbesplittedandexpressedintofactorpairsofa*, *Since* kx $\equiv a$ (mod p), all the numbers less than p have multiplicative inverse of each other with in this range. Thus $a^{\frac{p-1}{2}} = a \cdot a \cdots a = 1 \cdot 2 \cdots (p-1) = (p-1)!$

Also $(p-1)! = -1$ (By Wilson's Theorem).
Thus

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$$

. ■

Case 2 Illustration: Take $a = 3$ and $p = 7$. Finding all the factor pairs less than 7 in terms of 3 we get: $1 \cdot 3 \equiv 3, \quad 2 \cdot 5 \equiv 3, \quad 4 \cdot 6 \equiv 3 (\text{mod } 7)$.
Now , $3^{\frac{7-1}{2}} = 3^3 = 3 \cdot 3 \cdot 3 = (1 \cdot 3)(2 \cdot 5)(4 \cdot 6) = 1(3 \cdot 5)(2 \cdot 4)6 \equiv 6 \equiv -1 (\text{mod } 7)$

Properties:

Here are three important properties of the Legendre symbol

Theorem 2.2.1. *Let p be an odd prime with $p \nmid a$ and $p \nmid b$ then:*
1. $(\frac{a^2}{p})$ *= -1* *2.* $(\frac{a}{p}) = (\frac{b}{p})$ *if* $a \equiv b$ *(mod p)* *3.* $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$

Proof. 1. It is direct proof that follows from definition of Legendre symbol. Since a is a Q.R. (mod p). Then obviously a^2 is a Q.R. (mod p)

2. Since $a \equiv b$, then $x^2 \equiv a$ (mod p) has a solution if and only if $x^2 \equiv b$ (mod p) has a solution. Thus,

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

3. By Euler's criterion, we have

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{\text{p}}$$

Similarly,

$$\left(\frac{b}{p}\right) = b^{\frac{p-1}{2}} \pmod{\text{p}}$$

Hence we obtain

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{\text{p}}$$

Now let's see what are the conditions required for an integer to become Q.R. of a prime number. We will be looking at one positive integer and one negative integer.

Theorem 2.2.2. *For all odd prime p we have*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ (mod 4)} \\ -1 & \text{if } p \equiv -1 \text{ (mod 4)} \end{cases}$$

Proof : By Euler's criterion, we have

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{\text{p}}$$

Now, if $p \equiv 1 \pmod 4 = 4 \mid (p-1)$, then p= 4k+1 for some integer k. Thus

$$(-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$$

Similarly, if $p \equiv -11 \pmod 4 = 4 \mid (p-3)$, then p= 4k+3 for some integer k. So,

$$(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$$

■

Theorem 2.2.3. *For all odd prime p we have*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \text{ (mod 8)} \\ -1 & \text{if } p \equiv \pm 3 \text{ (mod 8)} \end{cases}$$

Proof. This prove is a bit tricky proof which we start by taking product of all $\frac{p-1}{2}$ congruences modulo p such that

$$\begin{aligned} p-1 &\equiv 1 \cdot (-1)^1 \pmod{\text{p}} \\ 2 &\equiv 2 \cdot (-1)^2 \pmod{\text{p}} \\ p-3 &\equiv 3 \cdot (-1)^3 \pmod{\text{p}} \\ 4 &\equiv 4 \cdot (-1)^4 \pmod{\text{p}} \\ &\vdots \\ s &\equiv \frac{p-1}{2} \cdot (-1)^{\frac{p-1}{2}} \pmod{\text{p}} \end{aligned}$$

where s is $\frac{p-1}{2}$. Taking product we now obtain,

$$(p-1)\cdots 6.4.2 \equiv \left(\frac{p-1}{2}\right)! * (-1)^{1+2+\cdots+\frac{p-1}{2}} \pmod{\text{p}}$$

This is equivalent as

$$\left(\frac{p-1}{2}\right)! * 2^{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)! * (-1)^{(p^2-1)/8}$$

where $(p^2-1)/8$ can be obtained using the summation of n numbers formula. Now we can cancel $\left(\frac{p-1}{2}\right)!$ from both sides and we get,

$$2^{\frac{p-1}{2}} \equiv (-1)^{(p^2-1)/8} \pmod{\text{p}}$$

Now, using Euler's Criterion, LHS is equal to

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p}$$

Thus, $(-1)^{(p^2-1)/8}$ is 1 (if $p \equiv \pm 1 \pmod 8$) and -1 (if $p \equiv \pm 3 \pmod 8$). ■

Gauss's Lemma:

Let p be a odd prime with $p \nmid a$. Let n denotes number of least positive residues of $a, 2a, 3a, \cdots \frac{p-1}{2}a$ that are greater than $\frac{p}{2}$. Then

$$\left(\frac{a}{p}\right) = (-1)^n$$

Proof. Consider the least residues of set S=$a, 2a, 3a, \cdots \frac{p-1}{2}a$
Let $r_1, \cdots, r_n$ = Numbers from S that are greater than $\frac{p}{2}$and $s_1, \cdots, s_m$ = Numbers from S that are less than $\frac{p}{2}$. Now consider, $p - r_1, p - r_2, \cdots p - r_n, s_1, \cdots, s_m$ that has exactly $\frac{p-1}{2}$ member and let's claim all these integers are different. Assume $p - r_i \equiv s_j \pmod p$, then

$$-r_i \equiv s_j \pmod p.$$

Now since all $r_i's$ and $s_j's$ are the multiple of a. Thus we can write it as $-k_i.a \equiv k_j.a \pmod p$. So, $k_i \equiv -k_j \pmod p$ which is a contradiction. Since this k is from 1 to (p-1), thus it won't be negative in case we take $\frac{p-1}{2}$. So our claim is inconsistent. Thus the list above is same as numbers from 1 to $\frac{p-1}{2}$. So,

$$p - r_1, \cdots, p - r_n, s_1, \cdots, s_m = 1, \cdots \frac{p-1}{2}$$

Multiplying terms in RHS and LHS we get,

$$(p - r_1) \cdots (p - r_n) s_{1m} \equiv \left(\frac{p-1}{2}\right)!$$

$$-r_1 \cdots - r_m \cdot s_1 \cdots s_m \equiv \left(\frac{p-1}{2}\right)!$$

$$(-1)^n \cdot r_1 \cdots r_n \cdot s_1 \cdots s_m \equiv \left(\frac{p-1}{2}\right)!$$

Now since $(r_1 \cdots r_n . s_1 \cdots s_m)$ is same as product of S, it is equal to $a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$

$$(-1)^n \cdot a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!$$

Now, after cancelling the terms we get, $(-1)^n \equiv a^{\frac{p-1}{2}}$. Hence by Euler's Criterion,

$$\left(\frac{a}{p}\right) = (-1)^n$$

■

2.3 Representation of integers in any base

Introduction:

Normally we use decimal systems in our daily life to represent integers. In this section, we will have a closer look on how we can write any positive integers in terms of any positive base integer. Mathematicians introduced this concept to see how numeric bases work. Nowadays, it is widely used in computers often called as binary language. Using decimal system makes circuits more complex and expensive, so computers use base-2 or base-8 because it is easier to implement them in electronic technology. Historically there have been several bases for representing numbers:
2: known as binary, widely use in computer;
8: known as octal, also used in computer;
10: known as decimal, used in daily life;
16: known as hexadecimal, used in ancient China;
20: known as vigesimal, used in ancient France (numbers 70-79 are counted as 60+10 to 60+19 in French, and 4*20 is 80)
60: sexagesimal, used by the Babylonians

Notation: An integer a represented in base b expansion is written as $(a)_b$

Generalization:

Assume b be a positive integer with b>1. Then any positive integer n can be expressed uniquely as

$$n = a_x b^x + a_{x-1} b^{x-1} + ... + a_1 b + a_0$$

where x is a positive integer, $0 \leq a_k < b$ for k= 0,1,..,x and $a_x \neq 0$

Proof : We will prove this theorem in two parts. First we will prove the equation and wil will prove it's uniqueness. This proof directly follows from division algorithm which we proved in previous chapter. It states that if n and b are integers such that b>0, then there exist unique integers q_0 and a_0 such that,

$$n = bq_0 + a_0, \quad where \quad 0 \leq a_0 < b.$$

Now if $q_0 \neq 0$ then we will divide q_0 by b from which we get

$$q_0 = bq_1 + a_1, \quad where \quad 0 \leq a_1 < b,$$

After continuing this process we will get sequence of such equations

$$q_1 = bq_2 + a_2, \quad where \quad 0 \leq a_2 < b,$$

.

.

.

$$q_{x-2} = bq_{x-2} + a_{x-1}, \quad where \quad 0 \leq a_{x-1} < b,$$

.

$$q_{x-1} = b.0 + a_x, \quad where \quad 0 \leq a_x < b,$$

From here we can observe that sequence $q_0, q_1, ...$ is a sequence of positive numbers which keeps on decreasing until last term q_x is 0.
Now we will substitute the equation $q_0 = bq_1 + a_1$ in $n = bq_0 + a_0$, to get

$$n = b(bq_1 + a_1) + a_0 = b^2q_1 + a_1b + a_0,$$

Now we can sense that we can again substitute the value of $q_1, q_2, .., q_{x-1}$ in m. From this we get

$$n = b^3q_2 + a_2b^2 + a_1b + a_0,$$

.

.

$$= b^xq_{x-1} + a_{x-1}b^{x-1} + ... + a_1b + a_0,$$
$$= a_xb^x + a_{x-1}b^{x-1} + ...a_1b + a_0,$$

Thus we can see that this has completed the first part of the proof. Now we need to prove that the representation is unique for each integer, which we will prove using contradiction.
Suppose now that for the same number there are different expansions. Let two expansions be

$$n = a_xb^x + a_{x-1}b^{x-1} + ...a_1b + a_0 = z_xb^x + z_{x-1}b^{x-1} + ...z_1b + z_0$$

Subtracting the two expansions we should get

$$(a_x - z_x)b^x + (a_{x-1} - z_{x-1})b^{x-1} + ...(a_1 - z_1)b + (a_0 - z_0) = 0$$

For these two expansions to be different the must exist $0 \leq k \leq x$ such that $z_k \neq a_k$ and now we get,

$$b^k((a_x - z_x)b^{x-k} + ... + (a_{k+1} - z_{k+1}b + (a_k - c_k)) = 0$$

and we know since $b \neq 0$, the next part must be zero. So we get

$$(a_x - z_x)b^{x-k} + ... + (a_{k+1} - z_{k+1})b + (a_k - c_k) = 0$$

Followed by this we get,

$$(a_x - z_x)b^{x-k} + ... + (a_{k+1} - z_{k+1})b = a_k - c_k$$

Taking common b from L.H.S and using concept of divisibility we get, $b|(a_k - z_k)$. Since $0 \leq a_k < b$ and $0 \leq z_k < b$, we get $a_k = z_k$ which is a contradiction since we assumed $z_k \neq a_k$. Thus we can say the expansion is unique.

Basic Examples:

Example 1:

Find the base 3 expansion of 619.

Sol : Using the expansion just like we did above. We have,

$$\begin{aligned} 619 &= 3*206+1 \\ 206 &= 3*68+2 \\ 68 &= 3*22+2 \\ 22 &= 3*7+1 \\ 7 &= 3*2+1 \\ 2 &= 3*0+2 \end{aligned}$$

Now taking the remainders from last gives us the expansion:

$$619 = (211221)_3$$

The next example will compel us to think about other application of expansion which will break down complex mathematical problems into simpler form. Let's take a look at how it works in modular exponentiation from example below .

Example 2:

Find the remainder when 4^{405} is divided by 235.

Sol : We will start by converting 405 in binary form and expressing it as a sum of powers of 2,

$$405 = (110010101)_2 = 2^8 + 2^7 + 2^4 + 2^2 + 2^0$$

Now we need to calculate the squares of 4 for 8,7,4,2 ,and 0 (mod 235:)

$$4^{2^0} = 4(\text{mod } 235),$$

$$4^{2^2} = 256 \equiv 21(\text{mod } 235),$$

$$4^{2^4} \equiv 206^2 \equiv 136(\text{mod } 235),$$

$$4^{2^7} \equiv 61^2 \equiv 196(\text{mod } 235),$$

$$4^{2^8} \equiv 196^2 \equiv 111(\text{mod } 235).$$

Thus we will get,

$$\begin{aligned} 4^{405} &= 4^{2^8+2^7+2^4+2^2+2^0} = 4^{2^8} * 4^{2^7} * 4^{2^4} * 4^{2^2} * 4^{2^0} \\ &\equiv 111 * 196 * 136 * 21 * 4 \equiv 79(\text{mod } 235). \end{aligned}$$

CHAPTER 3

Arithmetic Functions

Definition 3.0.1. An arithmetic functions or number-theoretic functions are real or complex valued functions defined over the positive integers. T

From the definition we can conclude that the domain is the positive integers, $\mathbb{Z}^+$, and the range is a subset of complex numbers, $\mathbb{C}$. An example of arithmetic functions is the divisors function which gives of an integer n the number of divisors of n.

Example 3.0.1. The following are some examples of trivial but powerful arithmetic functions:

$$\text{The identity function } I(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

$$\text{divisor function } \tau(n) = \sum_{d|n} 1$$

$$\text{Euler totient function } \phi(n) = \sum_{1 \le k \le n, (k,n)=1} 1$$

$$\text{Möbius function } \mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^r & \text{if } n = p_1 p_2 \cdots, p_j \text{ with } n \text{ is square-free,} \\ 0 & \text{otherwise} \end{cases}$$

Along this chapter, you will learn more about all of these function and more about their properties.

3.1 Multiplicative functions

Definition 3.1.1. An arithmetic function f which is not identically zero is said to be multiplicative if

$$f(mn) = f(m)f(n)$$

whenever $(m, n) = 1$

Theorem 3.1.1. *If f is multiplicative then f(1)=1*

Proof. We can say that $f(n) = f(n)f(1)$ from the definition of multiplicative functions. So, because f is not identically zero, $f(1) = 1$. ■

Here are some examples of multiplicative functions:

Theorem 3.1.2. *If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then we define the divisors function as follows*

$$\tau(n) = \prod_{i=1}^{r} (a_i + 1)$$

Proof. If $d|n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then $d = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$, where $0 \leq b_i \leq a_i \forall 1 \leq i \leq r$. So, the total number of ways to make d is $(a_1 + 1)(a_2 + 1) \cdots (a_r + 1)$. We can conclude the following formula:

$$\tau(n) = \prod_{i=1}^{r} (a_i + 1)$$

■

Corollary 3.1.1. *The divisor function, $\tau(n)$, is multiplicative.*

This corollary can be easily noticed from the definition of $\tau(n)$. We encourage you to stop and try to prove this rigorously.

Example 3.1.1.

n	1	2	3	5	10	30
$\tau(n)$	1	2	2	2	4	8

Theorem 3.1.3. *If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then we define the sum of divisors function as follows:*

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1}$$

Proof. If $d|n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then $d = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$, where $0 \leq b_i \leq a_i \forall 1 \leq i \leq r$. So, we can say that:

$$\sum_{d|n} d = \sum_{0 \leq b_i \leq a_i} \prod_{1 \leq i \leq r} p^{b_i} = \sum_{b_1=0}^{a_1} \sum_{b_2=0}^{a_2} \cdots \sum_{b_r=0}^{a_r} \prod_{i=1}^{r} {p_i}^{b_i}$$

This sum of products can be expressed as a product of the sums. So,

$$\sum_{b_1=0}^{a_1} \sum_{b_2=0}^{a_2} \cdots \sum_{b_r=0}^{a_r} \prod_{i=1}^{r} {p_i}^{b_i} = \prod_{i=1}^{k} \left(\sum_{b_i=0}^{a_i} p_i^{b_i} \right)$$

This sum represents the sum of geometric series. So, we can conclude our results as follows:

$$\sigma(n) = \sum_{d|n} d = \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1}$$

■

Corollary 3.1.2. *The sum of divisors function, σ, is multiplicative.*

The proof of this statement is left for the reader. Here are some examples that can help you see why it is multiplicative.

Example 3.1.2.

n	1	2	3	5	10	28
$\sigma(n)$	1	3	4	6	18	56

You can make a very simple but important note here, which is $\sigma(p) = p + 1$ where p is a prime number. You can prove this obvious fact. There is also a consequence of this sum of divisors function.

Corollary 3.1.3. *If $n \in \mathbb{N}$ is a perfect number, then $\sigma(n) = 2n$*

This proof is left for the reader. You can see this fact by examining some simple example such as 6 or 28. Due to this beautiful corollary, mathematicians could deduce a way to find out perfect numbers.

Remark 3.1.1. Every perfect number ,n, can be expressed as $n = 2^{p-1}(2^p - 1)$ where both p and $(2^p - 1)$ are primes. When $(2^p - 1)$ is a prime, it is called a Mersenne prime. Mathematicians believe that there is an infinite number of Mersenne primes. You can note that whenever you find a Mersenne prime you can find a perfect number. By applying the previous equation we can get:

$$\sigma(n) = \frac{2^p - 1}{2 - 1} * \frac{(2^p - 1)^2}{2^p - 1 - 1} = 2^p(2^p - 1) = 2(2^{p-1}(2^p - 1)) = 2n$$

Definition 3.1.2.

$$\text{Möbius function } \mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^r & \text{if } n = p_1 p_2 \cdots, p_j \text{ with } n \text{ is square-free,} \\ 0 & \text{otherwise} \end{cases} \tag{3.1}$$

Theorem 3.1.4. *The function μ is multiplicative.*

This can be proved by simple casework here. We encourage the reader to stop and do this casework.

Example 3.1.3.

n	1	2	9	6	7007	8
$\mu(n)$	1	-1	0	1	0	0

Theorem 3.1.5. *If $n \geq 1$, then we can say*

$$\sum_{d|n} \mu(d) = I(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We will use a similar method to prove this theory as we used in the previous proof. If $d|n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then $d = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$, where $0 \leq b_i \leq a_i \forall 1 \leq i \leq r$.

$$\sum_{d|n} \mu(d) = \sum_{0 \leq b_i \leq a_i} \prod_{1 \leq i \leq r} p^{b_i} = \sum_{b_1=0}^{a_1} \sum_{b_2=0}^{a_2} \cdots \sum_{b_r=0}^{a_r} \mu\left(\prod_{i=1}^{r} {p_i}^{b_i}\right)$$

$$\sum_{d|n} \mu(d) = \sum_{0 \leq b_i \leq a_i} \prod_{1 \leq i \leq r} p^{b_i} = \sum_{b_1=0}^{a_1} \sum_{b_2=0}^{a_2} \cdots \sum_{b_r=0}^{a_r} \mu(p^{b_1})\mu(p^{b_2}) \cdots \mu(p^{b_r})$$

$$\sum_{d|n} \mu(d) = \prod_{i=1}^{r} \sum_{0 \leq b_i \leq a_i} \mu(p_i^{b_i}) = \prod_{i=1}^{r} (1 - 1) = 0$$

■

Theorem 3.1.6. *Suppose f and g are arithmetic functions and define a function F by $F(n) = \sum_{d|n, d>0} f(d) * g(n/d)$. If f and g are both multiplicative, then F is also multiplicative.*

Proof. Suppose that $n = X * Y, (X, Y) = 1$ where $X = x_1 \cdots x_a$ and $Y = y_1 \cdots y_b$.

$$\begin{aligned} F(x)F(Y) &= \sum_{x_i|X} f(x_i)g(\frac{X}{x_i}) * \sum_{y_j|Y} f(y_j)g(\frac{Y}{y_i}) \\ &= (f(1)g(X) + \cdots + f(X)g(1))(f(1)g(Y) + \cdots + f(Y)g(1)) \\ &= f(1)g(1)f(n)g(n) + \cdots + f(1)g(1)f(n)g(n) \\ &= f(1)g(n) + \cdots + g(1)f(n) \\ &= \sum_{d|n} f(n)g(\frac{n}{d}) \\ &= F(n) \end{aligned}$$

So, F is multiplicative if f and g are both multiplicative. ■

Theorem 3.1.7. *Let f, g, h be arithmetic functions. Then we can say that:*

$$\begin{aligned} f * g = g * f, & \qquad \textit{(Commutativity)} \\ (f * g) * h = f * (g * h), & \qquad \textit{(associativity)} \end{aligned}$$

Proof. From 3.1.6,

$$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}) = \sum_{n=ab} f(a)g(b) = (g * f)(n)$$

and

$$((f * g) * h)(n) = \sum_{n=mc} (f * g)(m)h(c) = \sum_{n=abc} (f)(a) * (g)(b) * h(c) = f * (g * h)$$

■

Definition 3.1.3. Möbius transformation of an arithmetic function f is $F = f * u$, which is

$$F(n) = \sum_{d|n} f(d).$$

Theorem 3.1.8 (Möbius inversion formula.)**.** *$F = f * u$ iff $f = F * \mu$.*

Proof. If $F = f * u$, then $F * \mu = (f * u) * \mu = f * (u * \mu) = f * I = f$. You can show the reverse direction easily. ■

PART II

The Second Part

CHAPTER 4

Continued Fractions

4.1 General Continued Fractions

Continued fraction in simple words is the process of representing a number in the form of integer and series of nested fractions. It is is an interesting way of representing rationals and irrational number in terms of such fraction. It's first practical application was made by Dutch mathematician, Christian Huygens in 1687. He wrote on paper on how convergents can be used to best approximate the gear ratios. Later many famous mathematicians were also attracted by continued fraction and have contributed some say in this topic including Euler, Gauss, Jacobi and so on. Continued fraction has got many applications out of which one of the most important is finding solution to the pell's Equation which we will discuss later in this chapter. There are mainly two types of continued fraction : Finite Continued fraction and Infinite Continued fraction. Let's look at Finite Continued Fraction.

Finite Continued Fraction: A finite continued fraction is the fraction in which it's numbers of term are known. It is generally written in the form: $[a_0; a_1, a_2, .., a_n]$

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}$$

Infinite Continued Fraction: An infinite continued fraction is the fraction in which it's numbers of terms are known. Just like finite continued It is generally written in the form: $[a_0; a_1, a_2, a_3...]$

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

where the letters a_0, a_1, a_2 are just independent variable. Letter a_0 donotes an integer whereas $a_1, a_2...$ denote the positive numbers.

Example : Calculate continued fraction of *a.* [2,1,1,1,3] and *b.* [1,2,1,2,..].

Sol : Here, just like above representations it equals:
a.

$$2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{3}}}}=\frac{29}{11}$$

b. Assume

$$x=1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+\cdots}}}$$

Since 1,2 is repeating we can write it as

$$x=1+\cfrac{1}{2+\cfrac{1}{x}}=1+\frac{1}{\frac{2x+1}{x}}=\frac{3x+1}{2x+1}$$

Now, x(2x+1)=3x+1
$2x^2+x=3x+1$
$2x^2-2x-1=0$ Solving the quadratic equation we get, $x=\frac{1\pm\sqrt{3}}{2}$ and since x cannot be negative, $x=\frac{1+\sqrt{3}}{2}$

Continued Fraction of Decimal: We know that every rational number can be expressed in decimal fraction that stops at one point or cycles over same number again and again. There are several methods of converting such number in continued fraction out of will we will discuss one of them.
Steps: From the whole decimal part write down only whole part before decimal point and write it in the CF list and then subtract it from original number if it's approximately 0 such that it brings rounding error end here. Else calculate 1/x and write down the whole part before decimal similar to above. Now keep on repeating this unless you get 0 and you'll get continued fraction. We will have a look at one of it's example.

Example : Continued Fraction of 2.125.
Sol : Whole part is 2 so first number is [2;...] Now subtracting 2 we get 0.125 and $\frac{1}{0.125}$ equals 8. Whole part is 8 so second number is [2;8] and since 8 doesn't have any decimal part it's 0. So continued fraction is $2.125=2+\frac{1}{8}=\frac{17}{8}$.

Continued Fraction of Square roots: Square root are different from decimal since it is never ending decimal and repeats same same number again and again after some number. Now let's learn about how can we find the continued fraction for any square root $\sqrt{n}$ Steps: First we need to figure it out which is the nearest square number less than n, find it's root and name it b. This number is the start of our continued fraction. Next you will subtract b from $\sqrt{n}$ and find it's inverse, i.e. $x=\frac{1}{\sqrt{n}-b}$. Now since we have term with square root in denominator we have to rationalize by multiplying ($\sqrt{n}$ +b) on denominator and numerator and simplify. Now will won't proceed further if we get the expression that is equal to square root plus the first integer. Else will use the expression we get before and start again from first step. This will help you to find

continued fraction of any square root. Let's look at the example.

Example : Continued Fraction of $\sqrt{7}$.
Sol : Here, nearest square number less than 7 is 4 and $sqrt4is2$. Now we get $\frac{1}{\sqrt{7}-2}$ and rationalizing this we get $\frac{1}{\sqrt{7}-2}\frac{\sqrt{7}+2}{\sqrt{7}+2} = \frac{2+\sqrt{7}}{3}$. Now nearest square number less than $\frac{2+\sqrt{7}}{3}$equals 1. Now applying similar steps as we did previously we get $\frac{1+\sqrt{7}}{2}$ which is again 1. Following steps until we get $\sqrt{7}+2$ we get [2;1,1,1,4] which equals $\frac{37}{14}$which is the required fraction.

4.2 Convergences

Now we will be looking at n^{th} convergent of continued fraction $[a_0; a_1, a_2, .., a_n]$ which is the value obtained by combining a_0 to the fractional part after a_n.
Let

$$p_o = a_0, p_1 = a_0a_1 + 1, q_0 = 1 and q_1 = a_1$$

such that $a_0 = \frac{p_0}{q_0}$ Also,

$$a_0 + \frac{1}{a_1} = \frac{a_0a_1 + 1}{a_1} = \frac{p_1}{q_1}$$

Theorem 1: Let $p_n = a_np_{n-1} + pn - 2$ and $q_n = a_nqn - 1 + q_{n-2}$ then for $n > 1$, n^{th} convergent to $[a_0; a_1, a_2, .., a_n]$ is given by $\frac{p_n}{q_n}$.

Proof : Using Induction for $n > 1$,

$$\begin{aligned}
[a_0, .., a_{n-1}, a_n] &= [a_0, .., a_{n-1}, \frac{1}{a_n}] \\
&= \frac{(a_{n-1} + \frac{1}{a_n})p_{n-2} + p_{n-3}}{(a_{n-1} + \frac{1}{a_n})q_{n-2} + q_{n-3}} \\
&= \frac{a_n(a_{n-1}p_{n-2} + p_{n-3}) + p_{n-2}}{a_n(a_{n-1}q_{n-2} + q_{n-3}) + q_{n-2}} \\
&= \frac{a_np_{n-1} + p_{n-2}}{a_nq_{n-1} + q_{n-2}} \\
&= \frac{p_n}{q_n} \quad QED
\end{aligned}$$

In simple words to understand it more:
Consider the continued fraction of $\frac{29}{11}$,

$$\frac{29}{11} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3}}}}$$

Now all these fractional value below are known as the value of convergents of $\frac{29}{11}$,

$$2, \quad 2+\frac{1}{1}, \quad 2+\frac{1}{1+\frac{1}{1}}, \quad 2+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}$$

Thus $\frac{2}{1}, \frac{3}{1}, \frac{5}{2}, \frac{8}{3}$ are the fractional value of above mentioned fraction respectively and are known as convergents of $\frac{29}{11}$ as the value of all these value are approximately equal to the value of $\frac{29}{11}$.

Theorem 2: In a continued fraction x=$[a_0, a_1, a_2, ..]$ and $t_n = [a_n, a_{n+1}]$ for $n \geq 0$, then

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}$$

Proof : Using simple proof of Induction, we can get that $x = \frac{p_{n-2}+t_n p_{n-1}}{q_{n-2}+t_n q_{n-1}}$. Then,

$$\begin{aligned} x - \frac{p_n}{q_n} &= \frac{p_{n-2}+t_n p_{n-1}}{q_{n-2}+t_n q_{n-1}} - \frac{p_n}{q_n} \\ &= \frac{q_n p_{n-1} + t_{n+1} p_n q_n - p_n q_{n-1} - t_{n+1} p_n q_n}{q_n(q_{n-1}+t_{n+1}q_n)} \\ &= \frac{q_n p_{n-1} - p_n q_{n-1}}{q_n(q_{n-1}+t_{n+1}q_n)} \\ &= \frac{(-1)^n}{q_n(q_{n-1}+t_{n+1}q_n)} \end{aligned}$$

Also we know that $t_{n+1} > a_{n+1}$, such that $q_{n-1} + t_{n+1}q_n > q_{n-1} + a_{n+1}q_n = q_{n+1}$. So, since the q_i are increasing we can say,

$$\left| x - \frac{p_n}{q_n} \right| = \frac{1}{q_n(q_{n-1}+t_{n+1}q_n)} < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2} \quad QED$$

These are some of the facts about convergents of continued fraction. Upcoming section will give us more idea about the wide range use of convergents. In the meantime you can have a look at unique conjectures about convergents and try to think about other unique properties of convergents of continued fractions.

Conjectures:
1. Of any two consecutive convergents in the simple continued fraction expansion of α, at least one satisfies the inequality $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$.

2. If α is irrational, there exist infinitely many fractions $\frac{p}{q}$ such that $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$

4.3 Diophantine approximation

Convergents of continued fraction can be used to solve diophantine equations especially of the form ax+bx=1. For that we will learn about unique Magic box. Similar to magic box, in this section we will explore about topics like Farey Sequence and all.

Farey Pair:

Farey Pair is an interesting pair of two non-negative reduced fraction $\frac{a}{b}$ and $\frac{c}{d}$ where $bc - ad = 1$. We can also say two fraction are farey pair if they have difference of $\frac{1}{bd}$.

Theorem: For $n \geq 1$, then the convergents $\frac{p_{n-1}}{q_{n-1}}$ and $\frac{p_n}{q_n}$ of continued fraction are a farey pair. Then,

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$$

Proof : Using Induction, we see that this statement for n=1. Now for $n \geq 1$, we will get

$$\begin{aligned} p_n q_{n-1} - p_{n-1} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-1} - p_{n-1}(a_n q_{n-1} + q_{n-2}) \\ &= p_{n-2} q_{n-1} - p_{n-1} q_{n-2} = -(-1)^{n-2} \\ &= (-1)^{n-1} \quad QED \end{aligned}$$

Magic Box:

Consider the following box and continued fraction of $\frac{29}{11}$. Try to figure out if there's any relation between them.

		2	1	1	1	3
0	1	2	3	5	8	29
1	0	1	1	2	3	11

Have you noticed anything interesting about 2×2 determinants ? Try to find the solution of equation 29x + 11y = 1 ?

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 5 & 8 \\ 2 & 3 \end{bmatrix}, \begin{bmatrix} 8 & 29 \\ 3 & 11 \end{bmatrix}$$

Here you can see that first row of the box is same as the values of continued fraction $\frac{29}{11}$ =[2,1,1,1,3] and the the next two columns are just the convergents of $\frac{29}{11}$. Also we can see that the all the matrixes have determinant either 1 or -1. This actually follows from the theorem that we proved in Farey Pair part. Similarly using the same concept we can also solve the equation 29x + 11y = 1. Since using determinant concept we can see that in matrix $\begin{bmatrix} 8 & 29 \\ 3 & 11 \end{bmatrix}$, it's determinant is 11*8 - 29*3 = 1. Thus, x=-3 and y=8.

This is really interesting right? We are able to find so many things with the help of a small box. Now let's look at how we can create this table to find the convergents of a fraction from values of continued fraction $\frac{a}{b} = [a_0, a_1, a_2, ...]$

So for the first row you just have to plug in all the values of continued fraction and then the initial matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ should always be there. Then for next convergents you can follow the following steps.

		a_0	a_1	a_2	.	.
0	1	p_0	p_1	p_2	.	.
1	0	q_0	q_1	q_2	.	.

Now for finding $p_0, p_0 = a_0 \times 1 + 0$. Similarly $p_1 = a_1 \times p_0 + 1$, $p_2 = a_2 \times p_1 + p_0$. The same way $q_0 = a_0 \times 0 + 1$, $q_1 = a_1 \times q_0 + 0$, $q_2 = a_2 \times q_1 + q_0$. Also, for solving ax+by= 1, you can find the solution using the second-last convergent in the magic box. Using this you can create magic box for any continued fraction and use it to find convergent of continued fraction and solution to diophantine equation ax+by =1.

4.4 Solutions to Pell's equation

Pell's Equation is an equation in the form of $x^2 - dy^2 = 1$, where 'd' is non-square positive number. For the case when d is in square, the solutions are trivial. Let's start this section with this case.

When 'd' is in square form: $x^2 - dy^2 = (x - ny)(x + ny) = 1$. Then $(x - ny) = \pm 1$ and $(x + ny) = \pm 1$. We can see that this system of equations yields only solutions $(\pm 1, 0)$ regardless of d. But we will especially be looking at cases when 'd' is non-square positive number.
Let $\frac{p_n}{q_n}$ be the convergents of continued fraction of $\sqrt{d}$ and r be the length of the period of the expansion, then:

1. If r is even, then all positive solutions of $x^2 - dy^2 = 1$ are given by $x = p_{nr-1}, y = q_{nr-1} : (n = 1, 2, ...)$
2. If r is odd, then all positive solutions of $x^2 - dy^2 = 1$ are given by $x = p_{2nr-1}, y = q_{2nr-1} : (n = 1, 2, ...)$
3. If (x_0, y_0) is least positive solution of $x^2 - dy^2 = 1$, then all positive solutions(x_n, y_n) are given by $(x_n + y_n\sqrt{d}) = (x_0 + y_0\sqrt{d})^n$

Super Magic box:

Since convergent of continued fraction of $\sqrt{d}$ is the solution of $x^2 - dy^2 = 1$, we need to become familiar with how we can find the continued fraction of $\sqrt{d}$. In this section we'll discuss about super magic box and how we can use it to find the solution of Pell's equation.
Consider the following box and continued fraction of $\sqrt{7}$. Try to figure out if you can get solution to the equation $x^2 - 7y^2 = 1$.

		0	2	1	1	2
		1	3	2	3	1
		2	1	1	1	4
0	1	2	3	5	8	37
1	0	1	1	2	3	14

Just like the concept we used in magic box we know that bottom two rows gives us the value of the convergents $\frac{p_n}{q_n}$. The above two rows helps to find out the values in 3^{rd} row. The 3^{rd} row are the values that creates continued fraction with first value being integer part and next are the values of periods which repeats. In the example above we see the period of $\sqrt{7}$ has 4 coefficients and using the definition above since it has even number of coefficients, the positive solutions of $x^2 - 7y^2 = 1$ are given by $x = p_{4n-1}$ and $y = q_{4n-1}$. Thus, 4^{th} convergent also should satisfies this equation. This gives $8^2 - 7 * 3^2 = 1$ which is actually true. Thus (x,y)=(8,3).
We have learnt how we can create last two rows from third row in previous magic box section. Now, to create the first three rows there are series of steps to follow. Consider the following box for calculating the value of $\sqrt{d}$:

		A_0	A_1	A_2	A_3	A_4
		B_0	B_1	B_2	B_3	B_4
		a_0	a_1	a_2	a_3	a_4
0	1	p_0	p_1	p_2	p_3	p_4
1	0	q_0	q_1	q_2	q_3	q_4

We will start with the value of $A_0 = 0$ and $B_0 = 1$. Then for values of a_n, $a_n = \lfloor \frac{\lfloor \sqrt{d} \rfloor + A_{n+1}}{B_n} \rfloor$. Now for value of A_{n+1}, $A_{n+1} = C_n \times B_n - A_n$ and $B_{n+1} = \frac{d-(A_{n+1})^2}{B_n}$. Using these steps mentioned and the steps mentioned in the section of magic box section above you can make super-magic box. Then you can create the above mentioned rule to find the position of solution of the Pell's Equation.