Math 221 Section 4 Winter 2025: lecture diary

Darij Grinberg

draft, March 13, 2025

(This is **NOT** a text or a set of notes. It is just an archive of what I write on my virtual blackboard in class. See `https://www.cip.ifi.lmu.de/~grinberg/t/24wd/24wd.pdf` for the actual notes.)

0. Preface

This is a course on **discrete mathematics**: the mathematics of finite, discrete objects, such as integers, finite sets. Integer sequences are also included even though they are infinite (since you only care about finite parts of them). We will not cover linear algebra or abstract algebra – while still discrete mathematics, these topics have their own classes.

The major topics we will cover in this course are

- **mathematical induction** and **recursion**;
- **elementary number theory** (divisibility, prime numbers, coprimality);
- basic **enumerative combinatorics** (counting and binomial coefficients);
- *I hope that time allows me:* basic **combinatorial game theory**.

We will not go very deep, nor will we be fully rigorous at all times (but mostly we will be). See the notes for references that elaborate on these topics.

Office hours (Korman 263):

- Tue 3:30PM–4:30PM;
- Wed 12:30–1:30PM.

1. Induction and recursion

1.1. The Tower of Hanoi

1.1.1. The puzzle

The **Tower of Hanoi** is a nice and illustrative puzzle.

You have 3 pegs (or rods) rising from a table. The first peg has n disks stacked on it. The n disks have n different sizes, and they are stacked in the order of their sizes (largest disk at the bottom, smallest at the top).

You can make a certain kind of moves ("**Hanoi moves**"): You can take the topmost disk from one peg and put it on top of another peg. However, you can only do this if this disk is smaller than the other disks currently on that other peg. So you are not allowed to ever put a larger disk on top of a smaller one.

Your **goal** is to move all n disks onto the third peg.

This game can be played online (see a link in the notes).

1.1.2. Some experiments

In the case $n = 3$, we can find a winning strategy just by guessing around ("brute force"):

1. Move the smallest disk from peg 1 to peg 3.
2. Move the middle disk from peg 1 to peg 2.
3. Move the smallest disk from peg 3 to peg 2.
4. Move the largest disk from peg 1 to peg 3.
5. Move the smallest disk from peg 2 to peg 1.
6. Move the middle disk from peg 2 to peg 3.
7. Move the smallest disk from peg 1 to peg 3.

This wins the game in 7 moves. But of course, we can still ask:

Question 1.1.1. (a) Can we always win the game (for any n, not just 3)?
(b) If so, then what is the smallest # of moves we need to make?

Let us record the answers for small values of n:

- For $n = 0$, we win in 0 moves.
- For $n = 1$, we win in 1 move.

- For $n = 2$, we win in 3 moves.
- For $n = 3$, we win in 7 moves.
- For $n = 4$, we win in 9? 12? 13? 15? 20? moves? Or not at all?

Let us study these things more systematically.

1.1.3. The numbers m_n

Definition 1.1.2. For any integer $n \geq 0$, we let m_n denote the # of moves needed to win the Tower of Hanoi game with n disks. If the game cannot be won, then we set $m_n := \infty$.

So we found the following values of m_n:

n	0	1	2	3	4	5	6	7	8
m_n	0	1	3	≤ 7					

But finding m_4 by brute force (i.e., trying all possibilities) would be rather time-consuming. Instead, we try to look back at our winning strategy for $n = 3$ (the one that gave us $m_3 \leq 7$). It is not a random sequence of moves. Rather, it can be broken up into three subsequences:

- First, move the smaller two disks on peg 2. (This is a Tower of Hanoi puzzle for $n = 2$, which takes three moves.)
- Then, move the large disk on peg 3. (This is just a single move.)
- Then, move the smaller two disks from peg 2 to peg 3. (This is a Tower of Hanoi puzzle for $n = 2$, which takes three moves.)

Inspired by this, we can construct a move sequence that wins the Tower of Hanoi puzzle for $n = 4$:

- First, move the smaller three disks on peg 2. (This is a Tower of Hanoi puzzle for $n = 3$, which takes seven moves.)
- Then, move the large disk on peg 3.
- Then, move the smaller three disks from peg 2 to peg 3.

This gives a winning solution in 15 moves.

So $m_4 \leq 15$. We cannot yet claim that $m_4 = 15$ because we don't know whether this is a shortest possible winning solution: who tells us that we couldn't win faster?

n	0	1	2	3	4	5	6	7	8
m_n	0	1	3	≤ 7	≤ 15	≤ 31	≤ 63	≤ 127	≤ 255

.

Proposition 1.1.3. Let n be a positive integer. If m_{n-1} is an integer (i.e., not ∞), then $m_n \leq 2m_{n-1} + 1$.

Proof. Assume that m_{n-1} is an integer. Thus, we can win the game for $n-1$ disks in m_{n-1} moves. Let S be the strategy that does this. So the strategy S moves $n-1$ disks from peg 1 onto peg 3 in m_{n-1} moves.

Let S_{23} be the same strategy as S, but with the roles of pegs 2 and 3 swapped. Thus, this strategy S_{23} moves $n-1$ disks from peg 1 onto peg 3 in m_{n-1} moves.

Let S_{12} be the same strategy as S, but with the roles of pegs 1 and 2 swapped. Thus, this strategy S_{12} moves $n-1$ disks from peg 1 onto peg 2 in m_{n-1} moves.

Now, we proceed as follows to win the game with n disks:

1. We use the strategy S_{23} to move the $n-1$ smaller disks from peg 1 onto peg 2.
2. We move the largest disk from peg 1 onto peg 3.
3. We use the strategy S_{12} to move the $n-1$ smaller disks from peg 2 onto peg 3.

In total, this new strategy requires $m_{n-1} + 1 + m_{n-1} = 2m_{n-1} + 1$ moves. So we can win the game for n disks in $2m_{n-1} + 1$ moves. Thus, $m_n \leq 2m_{n-1} + 1$. □

Now, let us see that this inequality $m_n \leq 2m_{n-1} + 1$ is actually an equality – i.e., that we cannot win the game any faster than the above strategy allows us.

Proposition 1.1.4. Let n be a positive integer. If m_{n-1} is an integer (i.e., not ∞), then $m_n = 2m_{n-1} + 1$.

Proof. Assume that m_{n-1} is an integer. We already know that $m_n \leq 2m_{n-1} + 1$, so we only need to show that $m_n \geq 2m_{n-1} + 1$. In other words, we need to show that **any** strategy to win the game for n disks needs at least $2m_{n-1} + 1$ moves.

To show this, we consider any strategy to win the game for n disks.

At some point during this strategy, the largest disk has to move. Consider the **first** move in which this happens. Call this the "special move".

Before the special move can happen, the largest disk must be freed – i.e., all the $n-1$ smaller disks must be removed. Moreover, in order for the special move to happen, there has to be at least one free peg. Thus, in order for the special move to happen, all the $n-1$ smaller disks must have been moved onto another peg (all on the same peg). Achieving this is just a Tower of Hanoi game for $n-1$ disks, so it needs m_{n-1} many moves. Thus, we must have already made m_{n-1} many move before the special move.

After the special move, the largest disk is on one peg, whereas all the $n-1$ smaller disks are on another. To win the game, we need to move the latter to the peg with the former. That is yet another Tower of Hanoi game for $n-1$ disks that we need to win, and as we know, it takes m_{n-1} steps.

Thus, altogether, our strategy must have involved m_{n-1} steps before the special move; then the special move (1 step); and then m_{n-1} steps again, for a total of $m_{n-1}+1+m_{n-1} = 2m_{n-1}+1$ steps. Thus, $m_n \geq 2m_{n-1}+1$, and the proof is complete. □

This proposition allows us to recursively compute m_n for each number n,

n	0	1	2	3	4	5	6	7	8
m_n	0	1	3	7	15	31	63	127	255

.

Thus, the formula $m_n = 2m_{n-1}+1$ is called a **recursive formula** for the numbers m_n. Generally, a recursive formula means a formula that expresses m_n in terms of the previous values $m_0, m_1, \ldots, m_{n-1}$.

What about an explicit formula? One of you made a guess:

$$m_n \stackrel{?}{=} 2^n - 1.$$

How would we prove such a guess?

1.2. The Principle of Mathematical Induction

The easiest way to prove such a guess is by a method called **proof by induction** or just **(mathematical) induction**, and it relies on the following principle:

Theorem 1.2.1 (Principle of Mathematical Induction)**.** Let b be an integer.

Let $P(n)$ be a mathematical statement defined for each integer $n \geq b$. (For instance, $P(n)$ could be "$n+1 > n$" or "n is even" or "n is odd" or "n is prime" or "there exists a prime number than n". In particular, it does not have to be a true. So $P(n)$ is just a statement that depends on n; such a statement is called a **predicate** in logic.)

Assume the following:

1. The statement $P(b)$ holds (i.e., the statement $P(n)$ holds when $n = b$).
2. For each integer $n \geq b$, the implication $P(n) \Longrightarrow P(n+1)$ holds (i.e., if $P(n)$ holds, then $P(n+1)$ holds).

Then, the statement $P(n)$ holds for every integer $n \geq b$.

Before we discuss the meaning of this principle, let me show how to prove our $m_n = 2^n - 1$ claim using it. First I state it as a theorem:

Theorem 1.2.2 (explicit answer to Tower of Hanoi)**.** For each integer n, we let m_n be the # of steps needed to win the Tower of Hanoi game with n disks (or ∞ if the game cannot be won). Then,

$$m_n = 2^n - 1 \qquad \text{for each integer } n \geq 0.$$

Proof. We denote the statement "$m_n = 2^n - 1$" by $P(n)$. So we must prove that $P(n)$ holds for each integer $n \geq 0$.

According to the Principle of Mathematical Induction (applied to $b = 0$), we will achieve this once we can show that

1. the statement $P(0)$ holds;
2. for each integer $n \geq 0$, the implication $P(n) \Longrightarrow P(n+1)$ holds.

Proving these two claims will be our two goals; we call them Goal 1 and Goal 2.

Goal 1 is easy: $P(0)$ is just saying that $m_0 = 2^0 - 1$, but this is clear since both sides are 0.

Now we try to prove Goal 2. Let $n \geq 0$ be an integer. We must prove the implication $P(n) \Longrightarrow P(n+1)$. To prove it, we assume that $P(n)$ holds. We need to prove that $P(n+1)$ holds as well.

By assumption, $P(n)$ holds, i.e., we have $m_n = 2^n - 1$.

Our goal is to show that $P(n+1)$ holds, i.e., that we have $m_{n+1} \stackrel{?}{=} 2^{n+1} - 1$.

Can we express m_{n+1} in terms of m_n ?

The previous proposition tells us that $m_n = 2m_{n-1} + 1$ if $n \geq 1$. Applying it to $n+1$ instead of n, we obtain $m_{n+1} = 2m_n + 1$. Thus,

$$\begin{aligned} m_{n+1} &= 2 \underbrace{m_n}_{=2^n-1} + 1 = 2\left(2^n - 1\right) + 1 \\ &= \underbrace{2 \cdot 2^n}_{=2^{n+1}} \underbrace{-2+1}_{=-1} = 2^{n+1} - 1. \end{aligned}$$

In other words, $P(n+1)$ holds. Thus, we have proved $P(n+1)$ under the assumption that $P(n)$ holds. In other words, we have proved the implication $P(n) \Longrightarrow P(n+1)$.

So Goal 2 is achieved. Now that we have achieved both goals, the Principle of Mathematical Induction automatically guarantees that $P(n)$ holds for each integer $n \geq 0$. In other words, $m_n = 2^n - 1$ for each $n \geq 0$. Theorem proved. $\square$

How did this proof work? What is the logic underlying the Principle of Mathematical Induction?

Let's try to work by hand. Our goal was to show that $P(n)$ holds for $n \geq 0$. We have shown that $P(0)$ holds, and that $P(n) \implies P(n+1)$ holds for each $n \geq 0$. The latter means that $P(0) \implies P(1)$ and $P(1) \implies P(2)$ and $P(2) \implies P(3)$ and so on, i.e., that we have an infinite chain of implications

$$P(0) \implies P(1) \implies P(2) \implies P(3) \implies \cdots.$$

The Principle of Mathematical Induction is saying that whenever you have such an infinite chain **and** know that its leftmost statement (in our case, $P(0)$) holds, then all the statements in the chain must hold. Common sense tells us that this is true – after all, the truth of $P(0)$ gets spread along the chain by the implications, so that eventually it "reaches" each $P(n)$.

In mathematics, common sense needs to be formalized. Strictly speaking, you cannot say "we prove something by following a chain of implications". This is why we need the Principle of Mathematical Induction.

The Principle of Mathematical Induction cannot really be proved; it is one of the axioms of mathematics (along with a bunch of others, such as $(A \text{ and } B) \implies A$ and so on). The best you can do is derive this principle from another principle which some might consider more fundamental, but is essentially "on the same level".

1.3. Some more proofs by induction

A proof that uses the Principle of Mathematical Induction is called an **induction proof** (or **inductive proof**, or **proof by induction**). An example was our above proof of $m_n = 2^n - 1$. Let's see some more examples.

1.3.1. The sum of the first n positive integers

Theorem 1.3.1 ("Little Gauss formula"). For every integer $n \geq 0$, we have

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

The LHS here is understood to be the sum of the first n positive integers. For $n = 0$, this sum is an empty sum (i.e., it has no addends at all), and so its value is 0 by definition.

First proof of the Little Gauss formula. We set

$$s_n := 1 + 2 + \cdots + n \qquad \text{for each } n \geq 0.$$

Thus, we must prove that

$$s_n \stackrel{?}{=} \frac{n\left(n+1\right)}{2} \qquad \text{for each } n \geq 0.$$

Let us denote the statement "$s_n \stackrel{?}{=} \frac{n\left(n+1\right)}{2}$" by $P\left(n\right)$. So we need to prove that $P\left(n\right)$ holds for every $n \geq 0$.

According to the Principle of Mathematical Induction, it suffices to show that

1. the statement $P\left(0\right)$ holds;
2. for each $n \geq 0$, the implication $P\left(n\right) \Longrightarrow P\left(n+1\right)$ holds.

Goal 1 is easy: To prove $P\left(0\right)$, we must show that $s_0 = \frac{0\left(0+1\right)}{2}$, but this is just saying $0 = 0$ since s_0 is an empty sum.

Now to Goal 2. We let $n \geq 0$ be an integer, and we want to prove the implication $P\left(n\right) \Longrightarrow P\left(n+1\right)$. So we assume that $P\left(n\right)$ holds, and set out to prove that $P\left(n+1\right)$ holds.

By assumption, $P\left(n\right)$ holds, so that we have

$$s_n = \frac{n\left(n+1\right)}{2}.$$

We must prove $P\left(n+1\right)$; in other words, we must prove that

$$s_{n+1} \stackrel{?}{=} \frac{\left(n+1\right)\left(\left(n+1\right)+1\right)}{2}.$$

To do so, we observe that

$$\begin{aligned} s_{n+1} &= 1 + 2 + \cdots + \left(n+1\right) \\ &= \underbrace{1 + 2 + \cdots + n}_{=s_n} + \left(n+1\right) = \underbrace{s_n}_{= \frac{n\left(n+1\right)}{2}} + \left(n+1\right) \\ &= \frac{n\left(n+1\right)}{2} + \left(n+1\right) = \frac{n\left(n+1\right) + 2\left(n+1\right)}{2} \\ &= \frac{\left(n+2\right)\left(n+1\right)}{2} = \frac{\left(n+1\right)\left(n+2\right)}{2} = \frac{\left(n+1\right)\left(\left(n+1\right)+1\right)}{2}, \end{aligned}$$

which is what we need. So $P\left(n+1\right)$ is proved under the assumption of $P\left(n\right)$. In other words, we have proved the implication $P\left(n\right) \Longrightarrow P\left(n+1\right)$. So we have achieved Goal 2.

With both goals now achieved, we apply the Principle of Mathematical Induction to conclude that $P\left(n\right)$ holds for all $n \geq 0$, just as we desired. $\square$

Next time we will see many more such proofs, but also a second proof of the "Little Gauss formula" that does not use induction (at least not explicitly).

Lecture 2, 2025-01-09

Second proof of the Little Gauss formula. We have

$$\begin{aligned}
&2 \cdot (1+2+\cdots+n) \\
&= (1+2+\cdots+n) + (1+2+\cdots+n) \\
&= \quad 1+2+\cdots+n \\
&+ 1+2+\cdots+n \\
&= \quad 1+ \quad 2 \quad +\cdots+n \\
&+ n+(n-1)+\cdots+1 \\
&\qquad\qquad \left(\begin{array}{c}\text{here, we have reversed the order} \\ \text{of the last } n \text{ addends from } 1,2,\ldots,n \\ \text{to } n, n-1, \ldots, 1\end{array}\right) \\
&= \underbrace{(1+n)}_{=n+1} + \underbrace{(2+(n-1))}_{=n+1} + \cdots + \underbrace{(n+1)}_{=n+1} \\
&\qquad\qquad \left(\begin{array}{c}\text{here, we arranged our addends into pairs} \\ \text{by pairing each top addend with the one below it}\end{array}\right) \\
&= n\,(n+1) \qquad (\text{since there are } n \text{ addends, each of them } = n+1).
\end{aligned}$$

Divide by 2 and we're done. □

Both proofs have their pros and cons. The induction proof is very automatic and paint-by-numbers. The second proof requires a trick but with the trick is very memorable; it also lets you guess the formula and not just prove it.

1.3.2. The sum of the squares of the first n positive integers

Theorem 1.3.2. For every integer $n \geq 0$, we have

$$1^2 + 2^2 + \cdots + n^2 = \frac{n\,(n+1)\,(2n+1)}{6}.$$

Proof. The following proof is almost a word-by-word copy of the first proof of the Little Gauss formula.

We set

$$s_n := 1^2 + 2^2 + \cdots + n^2 \qquad \text{for each } n \geq 0.$$

Thus, we must prove that

$$s_n \stackrel{?}{=} \frac{n\,(n+1)\,(2n+1)}{6} \qquad \text{for each } n \geq 0.$$

Let us denote the statement "$s_n \stackrel{?}{=} \dfrac{n(n+1)(2n+1)}{6}$" by $P(n)$. So we need to prove that $P(n)$ holds for every $n \geq 0$.

According to the Principle of Mathematical Induction, it suffices to show that

1. the statement $P(0)$ holds;
2. for each $n \geq 0$, the implication $P(n) \Longrightarrow P(n+1)$ holds.

Goal 1 is easy: To prove $P(0)$, we must show that $s_0 = \dfrac{0(0+1)(2\cdot 0+1)}{6}$, but this is just saying $0 = 0$ since s_0 is an empty sum.

Now to Goal 2. We let $n \geq 0$ be an integer, and we want to prove the implication $P(n) \Longrightarrow P(n+1)$. So we assume that $P(n)$ holds, and set out to prove that $P(n+1)$ holds.

By assumption, $P(n)$ holds, so that we have

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

We must prove $P(n+1)$; in other words, we must prove that

$$s_{n+1} \stackrel{?}{=} \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}.$$

To do so, we observe that

$$\begin{aligned}
s_{n+1} &= 1^2 + 2^2 + \cdots + (n+1)^2 \\
&= \underbrace{1^2 + 2^2 + \cdots + n^2}_{=s_n} + (n+1)^2 = \underbrace{s_n}_{=\frac{n(n+1)(2n+1)}{6}} + (n+1)^2 \\
&= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
&= (n+1)\cdot\left(\frac{n(2n+1)}{6} + (n+1)\right) \\
&= (n+1)\cdot\frac{n(2n+1)+6(n+1)}{6} \\
&= \frac{(n+1)\left(2n^2+7n+6\right)}{6} \\
&= \frac{(n+1)\left(2n^2+4n+3n+6\right)}{6} \\
&= \frac{(n+1)(n+2)(2n+3)}{6} \\
&= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6},
\end{aligned}$$

which is what we need. So $P(n+1)$ is proved under the assumption of $P(n)$. In other words, we have proved the implication $P(n) \Longrightarrow P(n+1)$. So we have achieved Goal 2.

With both goals now achieved, we apply the Principle of Mathematical Induction to conclude that $P(n)$ holds for all $n \geq 0$, just as we desired. □

So much for the induction proof. What about the trick proof? Sadly, I don't know how to adapt it to the new theorem. While the trick has various other uses, here it doesn't lead us anywhere. But induction reliably works.

1.4. Notations for an induction proof

Here comes some standard terminology that is commonly used in proofs by induction. Let's say that you are proving a statement of the form $P(n)$ for every integer $n \geq b$ (where b is some fixed integer).

- The n is called the **induction variable**; you say that you **induct on** n. It can have any name, not necessarily n. For example, if your statement is "for every integer a, we have $1+2+\cdots+a = \dfrac{a(a+1)}{2}$", then you can prove it by inducting on a.
- The proof of $P(b)$ (that is, Goal 1 in our above proofs) is called the **induction base** or **base case**. In our above examples, b was 0, but it can be any integer. For example, if you are proving the statement "every integer $n \geq 4$ satisfies $2^n \geq n^2$", then b will have to be 4, so your base case will be proving that $2^4 \geq 4^2$.
- The proof of "$P(n) \Longrightarrow P(n+1)$ for every $n \geq b$" (that is, Goal 2 in our above proofs) is called the **induction step**. For example, in our proof of Little Gauss, this was the part where we assumed that $s_n = \dfrac{n(n+1)}{2}$ and showed that $s_{n+1} = \dfrac{(n+1)((n+1)+1)}{2}$.

  In the induction step, the assumption that $P(n)$ holds is called the **induction hypothesis** or **induction assumption**. The claim that $P(n+1)$ holds (this is the claim you are trying to prove) is called the **induction goal**. The induction step is complete when this goal is reached.

As an example, let us rewrite our induction proof of $m_n = 2^n - 1$ using this language:

Theorem 1.4.1 (explicit answer to Tower of Hanoi)**.** For each integer n, we let m_n be the # of steps needed to win the Tower of Hanoi game with n disks (or ∞ if the game cannot be won). Then,

$$m_n = 2^n - 1 \qquad \text{for each integer } n \geq 0.$$

Proof. We induct on n.

Base case: The theorem is true for $n = 0$, since $m_0 = 0 = 2^0 - 1$.

Induction step: Let $n \geq 0$ be an integer. We assume that the theorem holds for n (this is what we previously called $P(n)$). We will now show that the theorem holds for $n+1$ as well.

We assumed that the theorem holds for n. That is, we have $m_n = 2^n - 1$. In particular, m_n is an integer.

We must prove that the theorem holds for $n+1$. In other words, we must prove that $m_{n+1} \stackrel{?}{=} 2^{n+1} - 1$.

To prove this, we apply the preceding proposition to $n+1$ instead of n. Thus we obtain

$$\begin{aligned} m_{n+1} &= 2 \underbrace{m_n}_{\substack{=2^n-1 \\ \text{(by the induction} \\ \text{hypothesis)}}} + 1 = 2\left(2^n - 1\right) + 1 = \underbrace{2 \cdot 2^n}_{=2^{n+1}} - 2 + 1 \\ &= 2^{n+1} - 2 + 1 = 2^{n+1} - 1. \end{aligned}$$

Thus we have reached the induction goal. So the induction step is complete, and the theorem is proved. □

1.5. The Fibonacci numbers

Our next applications of induction will involve the **Fibonacci sequence**. This is a sequence of integers defined **recursively** – i.e., a given entry is defined not directly but rather in terms of the previous entries. Specifically, its definition is as follows:

Definition 1.5.1. The **Fibonacci sequence** is the sequence $(f_0, f_1, f_2, \ldots)$ of nonnegative integers defined recursively by setting

$$\begin{aligned} &f_0 = 0, \qquad f_1 = 1, \\ &f_n = f_{n-1} + f_{n-2} \qquad \text{for each } n \geq 2. \end{aligned}$$

In other words, the Fibonacci sequence starts with the two entries 0 and 1, and then each further entry is the sum of the two previous entries.

The entries of this sequence are called the **Fibonacci numbers**. Here are the first few:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233

.

As we see, a recursive definition is a perfectly valid way to define (e.g.) a sequence of numbers. It allows you to compute each entry of the sequence provided that you have computed all the previous entries. So you can find f_{17} by computing $f_0, f_1, \ldots, f_{16}, f_{17}$ in this order.

Let us show some simple properties of Fibonacci numbers:

Theorem 1.5.2. For any integer $n \geq 0$, we have

$$f_1 + f_2 + \cdots + f_n = f_{n+2} - 1.$$

For example, for $n = 7$, this is saying that

$$f_1 + f_2 + f_3 + f_4 + f_5 + f_6 + f_7 = 1 + 1 + 2 + 3 + 5 + 8 + 13 = 33;$$

for $n = 8$, this is saying that

$$f_1 + f_2 + f_3 + f_4 + f_5 + f_6 + f_7 + f_8 = 1 + 1 + 2 + 3 + 5 + 8 + 13 + 21 = 54.$$

Proof of the theorem. We induct on n.

Base case: For $n = 0$, the theorem claims that $f_1 + f_2 + \cdots + f_0 = f_{0+2} - 1$. The LHS is an empty sum (it ends before it has a chance to start), so equals 0 by definition. The RHS is $f_{0+2} - 1 = f_2 - 1 = 1 - 1 = 0$. So the base case is done.

Induction step: Let $n \geq 0$ be an integer. Assume that the theorem holds for n. We must prove that it also holds for $n + 1$.

So we assumed that

$$f_1 + f_2 + \cdots + f_n = f_{n+2} - 1.$$

We must prove that

$$f_1 + f_2 + \cdots + f_{n+1} \stackrel{?}{=} f_{(n+1)+2} - 1.$$

We have

$$\begin{aligned} f_1 + f_2 + \cdots + f_{n+1} &= \underbrace{\left(f_1 + f_2 + \cdots + f_n\right)}_{\substack{= f_{n+2} - 1 \\ \text{(by the induction hypothesis)}}} + f_{n+1} \\ &= \left(f_{n+2} - 1\right) + f_{n+1} = \underbrace{f_{n+2} + f_{n+1}}_{\substack{= f_{n+3} \\ \text{(by the recursive definition of the Fibonacci numbers)}}} - 1 \\ &= f_{n+3} - 1 = f_{(n+1)+2} - 1. \end{aligned}$$

This achieves our induction goal, thus completes the induction step, hence completes the proof. □

1.6. Some more examples of induction

Theorem 1.6.1. For any integer $n \geq 0$, we have

$$2^0 + 2^1 + \cdots + 2^{n-1} = 2^n - 1.$$

Proof. We induct on n.

Base case: For $n = 0$, the theorem claims that an empty sum is $2^0 - 1$, which is obvious (since 0 is 0).

Induction step: Let $n \geq 0$ be an integer. Assume that the theorem holds for n, i.e., that

$$2^0 + 2^1 + \cdots + 2^{n-1} = 2^n - 1.$$

We must prove that the theorem also holds for $n + 1$, i.e., that we have

$$2^0 + 2^1 + \cdots + 2^{(n+1)-1} \stackrel{?}{=} 2^{n+1} - 1.$$

But

$$\begin{aligned} &2^0 + 2^1 + \cdots + 2^{(n+1)-1} \\ &= 2^0 + 2^1 + \cdots + 2^n \\ &= \underbrace{\left(2^0 + 2^1 + \cdots + 2^{n-1}\right)}_{= 2^n - 1} + 2^n \\ &= 2^n - 1 + 2^n = \underbrace{2 \cdot 2^n}_{= 2^{n+1}} - 1 = 2^{n+1} - 1, \end{aligned}$$

qed (i.e., this is the induction goal; so the induction step is complete; thus the theorem is proved). □

More generally:

Theorem 1.6.2. Let x and y be any two numbers. Then, for any integer $n \geq 0$, we have

$$(x-y)\left(x^{n-1}+x^{n-2}y+x^{n-3}y^2+\cdots+x^2y^{n-3}+xy^{n-2}+y^{n-1}\right) = x^n - y^n.$$

Here, the big sum is the sum of all products $x^i y^j$ where i and j are nonnegative integers with $i+j = n-1$.

Before we prove this, we give some examples:

- For $n = 2$, this theorem says
$$(x-y)(x+y) = x^2 - y^2.$$
- For $n = 3$, this theorem says
$$(x-y)\left(x^2+xy+y^2\right) = x^3 - y^3.$$
- For $n = 4$, this theorem says
$$(x-y)\left(x^3+x^2y+xy^2+y^3\right) = x^4 - y^4.$$
- For $x = 2$ and $y = 1$, this theorem says
$$(2-1)\left(2^{n-1}+2^{n-2}1+2^{n-3}1^2+\cdots+2^2 1^{n-3}+2\cdot 1^{n-2}+1^{n-1}\right) = 2^n - 1^n.$$
This simplifies to
$$2^{n-1}+2^{n-2}+2^{n-3}+\cdots+2^2+2+1 = 2^n - 1.$$
In other words,
$$2^0+2^1+\cdots+2^{n-1} = 2^n - 1.$$
So the previous theorem is a particular case of this one.

Now it remains to prove this theorem.

Proof. We induct on n.
Base case: For $n = 0$, the claim
$$(x-y)\left(x^{n-1}+x^{n-2}y+x^{n-3}y^2+\cdots+x^2y^{n-3}+xy^{n-2}+y^{n-1}\right) = x^n - y^n$$
is true, since the big sum on the LHS is empty (thus $= 0$) whereas the RHS is $x^0 - y^0 = 1 - 1 = 0$.

Induction step: Let $n \geq 0$ be an integer. Assume that the theorem is true for n. That is, assume that

$$(x-y)\left(x^{n-1}+x^{n-2}y+x^{n-3}y^2+\cdots+x^2y^{n-3}+xy^{n-2}+y^{n-1}\right) = x^n - y^n.$$

We must prove that the theorem is also true for $n+1$. That is, we must prove that

$$(x-y)\left(x^{n}+x^{n-1}y+x^{n-2}y^2+\cdots+x^2y^{n-2}+xy^{n-1}+y^{n}\right) = x^{n+1} - y^{n+1}.$$

But

$$\begin{aligned}
&(x-y)\left(x^{n}+x^{n-1}y+x^{n-2}y^2+\cdots+x^2y^{n-2}+xy^{n-1}+y^{n}\right) \\
&= (x-y)\,x^n + (x-y)\underbrace{\left(x^{n-1}y+x^{n-2}y^2+\cdots+x^2y^{n-2}+xy^{n-1}+y^{n}\right)}_{=\left(x^{n-1}+x^{n-2}y+\cdots+x^2y^{n-3}+xy^{n-2}+y^{n-1}\right)y} \\
&= (x-y)\,x^n + \underbrace{(x-y)\left(x^{n-1}+x^{n-2}y+\cdots+x^2y^{n-3}+xy^{n-2}+y^{n-1}\right)}_{\substack{=(x-y)\left(x^{n-1}+x^{n-2}y+x^{n-3}y^2+\cdots+x^2y^{n-3}+xy^{n-2}+y^{n-1}\right) \\ =x^n-y^n \\ \text{(by our induction hypothesis)}}} y \\
&= (x-y)\,x^n + (x^n-y^n)\,y = x^{n+1} - yx^n + x^ny - y^{n+1} = x^{n+1} - y^{n+1}.
\end{aligned}$$

This completes the induction step, and thus proves the theorem. □

Corollary 1.6.3 (geometric sum formula)**.** Let q be a number distinct from 1. Let $n \geq 0$ be an integer. Then,

$$q^0 + q^1 + \cdots + q^{n-1} = \frac{q^n - 1}{q-1}.$$

Proof. Apply the previous theorem to $x = q$ and $y = 1$; then simplify. □

1.7. How not to use induction

Induction can be slippery:

Theorem 1.7.1 (Fake theorem)**.** In any set of $n \geq 1$ horses, all the horses are the same color.

Proof. We induct on n.

Base case: This is clearly true for $n = 1$, since a single horse always has the same color as itself.

Induction step: Let $n \geq 1$ be an integer. We assume that the theorem holds for n, i.e., that any n horses have the same color.

We must prove that it also holds for $n+1$, i.e., that any $n+1$ horses have the same color.

Consider $n+1$ horses $H_1, H_2, \ldots, H_{n+1}$.

By our induction hypothesis, the first n horses $H_1, H_2, \ldots, H_n$ have the same color.

Again by our induction hypothesis, the last n horses $H_2, H_3, \ldots, H_{n+1}$ have the same color.

Now consider the first horse H_1 and the last horse H_{n+1}. They both have the same color as the "middle horses" $H_2, H_3, \ldots, H_n$. So all the $n+1$ horses have the same color, right?

Let's debug this proof. Where exactly (i.e., for which n) does the theorem go wrong? For $n = 1$, it is still true, so the base case is not at fault. But the theorem is false for $n = 2$, so the induction step $P(n) \Longrightarrow P(n+1)$ must already fail for $n = 1$. How? In the $n = 1$ case, there are no "middle horses", so our argument about H_1 and H_{n+1} having the same color as these "middle horses" does not work. We implicitly assumed their existence because the notation $H_1, H_2, \ldots, H_{n+1}$ sort-of makes it look like they exist; but this notation is merely meant to give an idea of what is being listed, not saying that the list has at least four entries. □

Note that this error only appears in the $n = 1$ case, but it renders the proof invalid for all $n \geq 2$, since the chain $P(1) \Longrightarrow P(2) \Longrightarrow P(3) \Longrightarrow \cdots$ is broken at that step.

1.8. More on the Fibonacci numbers

Recall the table of Fibonacci numbers:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233

.

We prove some more of its properties:

Theorem 1.8.1 (addition theorem for Fibonacci numbers)**.** We have

$$f_{n+m+1} = f_n f_m + f_{n+1} f_{m+1} \qquad \text{for all } n, m \geq 0.$$

Proof. Can you induct on two variables at the same time? We can, if we nest the two inductions inside one another. Fortunately, this is rarely necessary. Case in point, in this theorem, it suffices to induct on one of the two variables.

Which one? Doesn't matter, since n and m play symmetric roles. So let's induct on n. To this purpose, for every integer $n \geq 0$, we define the statement $P(n)$ to say

"for all integers $m \geq 0$, we have $f_{n+m+1} = f_n f_m + f_{n+1} f_{m+1}$".

(Don't forget the "for all integers $m \geq 0$" part!)

We shall prove this statement $P(n)$ for all $n \geq 0$ by induction on n.

Base case: We must prove $P(0)$. In other words, we must prove that

"for all integers $m \geq 0$, we have $f_{0+m+1} = f_0 f_m + f_{0+1} f_{m+1}$".

But this can be done by hand:

$$\underbrace{f_0}_{=0} f_m + \underbrace{f_{0+1}}_{=f_1=1} f_{m+1} = 0 f_m + 1 f_{m+1} = f_{m+1} = f_{0+m+1}.$$

Induction step: Let $n \geq 0$ be an integer. We assume that $P(n)$ holds. We must show that $P(n+1)$ holds.

Our induction hypothesis is saying that $P(n)$ holds, i.e., that

"for all integers $p \geq 0$, we have $f_{n+p+1} = f_n f_p + f_{n+1} f_{p+1}$"

(indeed, we have renamed the variable m as p in this statement, since it has nothing to do with the m we are currently considering)

We must prove that $P(n+1)$ holds, i.e., that

"for all integers $m \geq 0$, we have $f_{n+1+m+1} = f_{n+1} f_m + f_{n+1+1} f_{m+1}$".

To prove this, let $m \geq 0$ be an integer. Then,

$$\begin{aligned}
&f_{n+1} f_m + \underbrace{f_{n+1+1}}_{\substack{=f_{n+2}=f_{n+1}+f_n \\ \text{(by the definition} \\ \text{of the Fibonacci sequence)}}} f_{m+1} \\
&= f_{n+1} f_m + \left(f_{n+1} + f_n\right) f_{m+1} \\
&= f_{n+1} f_m + f_{n+1} f_{m+1} + f_n f_{m+1} \\
&= f_{n+1} \underbrace{\left(f_m + f_{m+1}\right)}_{\substack{=f_{m+2} \\ \text{(by the definition} \\ \text{of the Fibonacci sequence)}}} + f_n f_{m+1} \\
&= f_{n+1} f_{m+2} + f_n f_{m+1} = f_n f_{m+1} + f_{n+1} f_{m+2}
\end{aligned}$$

For comparison, the IH (= induction hypothesis) says that

"for all integers $p \geq 0$, we have $f_{n+p+1} = f_n f_p + f_{n+1} f_{p+1}$".

Applying this to $p = m + 1$, we obtain

$$\begin{aligned} f_{n+(m+1)+1} &= f_n f_{m+1} + f_{n+1} f_{(m+1)+1} \\ &= f_n f_{m+1} + f_{n+1} f_{m+2} \\ &= f_{n+1} f_m + f_{n+1+1} f_{m+1} \qquad \text{(as we saw above)}. \end{aligned}$$

In other words,

$$f_{n+1+m+1} = f_{n+1} f_m + f_{n+1+1} f_{m+1}$$

(since $n + (m+1) + 1 = n + 1 + m + 1$). □

1.8.1. Divisibility of Fibonacci numbers

Definition 1.8.2. Let a and b be two integers. We say that a **divides** b (and we write $a \mid b$) if there exists an integer c such that $b = ac$. Equivalently, we say that b **is divisible by** a in this case.

For example, $2 \mid 4$ and $3 \mid 12$ but not $3 \mid 14$. Note that $0 \mid 0$ and $5 \mid 0$ but not $0 \mid 5$.

Theorem 1.8.3. If $a, b \geq 0$ are two integers that satisfy $a \mid b$, then $f_a \mid f_b$.

Proof. It is reasonable to try induction. However, induction on a is rather hopeless (there is no relation whatsoever between $a \mid b$ and $a + 1 \mid b$). Induction on b does not really work either, since $a \mid b$ usually precludes $a \mid b + 1$.

However, let's not give up. We can introduce a new variable and induct on that.

Indeed, the condition $a \mid b$ means that $b = ac$ for some integer $c \geq 0$ (since $a, b \geq 0$). So we can restate the claim of the theorem as follows: "If $a, b, c \geq 0$ are three integers that satisfy $b = ac$, then $f_a \mid f_b$". Or, eliminating the b, this can be rewritten as

"If $a, c \geq 0$ are two integers, then $f_a \mid f_{ac}$".

Now, **this** statement we can prove by induction on c:

Base case: For $c = 0$, this is simply saying that $f_a \mid f_{a \cdot 0}$, which is clear because $f_{a \cdot 0} = f_0 = 0$ is divisible by everything.

Induction step: Let $c \geq 0$ be an integer. We assume (as the IH) that

"If $a \geq 0$ is an integer, then $f_a \mid f_{ac}$".

We must prove that the same holds for $c + 1$ instead of c, i.e., that

"If $a \geq 0$ is an integer, then $f_a \mid f_{a(c+1)}$".

So let us prove this. Let $a \geq 0$ be an integer. We want to show that $f_a \mid f_{a(c+1)}$. Our induction hypothesis gives us $f_a \mid f_{ac}$. What now?

We have

$$\begin{aligned} f_{a(c+1)} &= f_{ac+a} = f_{ac+(a-1)+1} \\ &= \underbrace{f_{ac}}_{\substack{\text{divisible by } f_a \\ \text{(by the IH)}}} f_{a-1} + f_{ac+1} \underbrace{f_{(a-1)+1}}_{=f_a} \qquad \text{(by the addition formula)} \\ &= f_a \,(\text{something}) + (\text{something else})\, f_a, \end{aligned}$$

and this is obviously divisible by f_a. So we have shown that $f_a \mid f_{a(c+1)}$, and this completes the induction step.

.....

Does it? I claim there is a little (fixable) mistake in the above proof.

The structure of the proof is correct: Our restatement in terms of a, c is indeed equivalent to the theorem, and we are indeed allowed to induct on c. The base case is correct, too. In fact, we have applied the addition formula

$$f_{n+m+1} = f_n f_m + f_{n+1} f_{m+1} \qquad \text{for all } n, m \geq 0$$

to $n = ac$ and $m = a - 1$. But this requires $ac \geq 0$ and $a - 1 \geq 0$. Now, $ac \geq 0$ is clear. But $a - 1 \geq 0$ only if $a \neq 0$. So the above argument doesn't work for $a = 0$ (although it works for all other a's).

This makes it clear how to plug this hole: We just need an extra argument for the case $a = 0$. But this is very easy: If $a = 0$, then both f_a and f_{ac} are $f_0 = 0$, so the divisibility $f_a \mid f_{ac}$ is clearly satisfied.

We can easily embed this argument as a case distinction into the above induction step. □

1.8.2. Binet's formula

Is there an explicit formula for f_n, that is, a formula that does not rely on previous entries of the Fibonacci sequence? The answer is "yes", and it is called **Binet's formula**:

Theorem 1.8.4 (Binet's formula)**.** Let

$$\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618\ldots \qquad \text{and} \qquad \psi = \frac{1-\sqrt{5}}{2} \approx -0.618\ldots.$$

We have

$$f_n = \frac{\varphi^n - \psi^n}{\sqrt{5}} \qquad \text{for each integer } n \geq 0.$$

The number φ here is called the **golden ratio**, and is famous for its many properties, most importantly the fact that it solves the quadratic equation $x^2 = x + 1$. The other solution of this equation is ψ. Surprisingly, the irrationality of φ and ψ does not prevent the fraction $\dfrac{\varphi^n - \psi^n}{\sqrt{5}}$ from being an integer and actually being the Fibonacci number f_n.

Binet's formula shows that f_n grows exponentially with growth rate $\varphi \approx 1.618\ldots$.

We will soon see a proof of Binet's formula. We will not see a proper motivation for it; that can be found in courses on linear algebra or generating functions.

Let's try proving it by induction on n:

Attempted proof of Binet's formula. We induct on n:

Base case: For $n = 0$, we have

$$f_0 = \frac{\varphi^0 - \psi^0}{\sqrt{5}},$$

which is true because $f_0 = 0$ whereas $\varphi^0 - \psi^0 = 1 - 1 = 0$.

Induction step: Let $n \geq 0$ be an integer. Assume (as the IH) that Binet's formula holds for this n; we must prove that it holds for $n + 1$. So we must show that

$$f_{n+1} = \frac{\varphi^{n+1} - \psi^{n+1}}{\sqrt{5}}.$$

The recursive definition of the Fibonacci sequence yields

$$f_{n+1} = f_n + f_{n-1} = \frac{\varphi^n - \psi^n}{\sqrt{5}} + f_{n-1} \qquad \text{(by the IH)}.$$

Unfortunately, we cannot really do anything with the f_{n-1} term: Our IH is only about n, not about $n - 1$. □

So we are stuck because our induction does not have "a long memory": Proving the claim for $n + 1$, we are assuming it only for n, not for $n - 1$ or for any older value.

For this purpose, there is a more advanced version of induction called **strong induction**.

1.9. Strong induction

1.9.1. Reminder on regular induction

The regular (original) principle of induction stated:

Theorem 1.9.1 (Principle of Mathematical Induction)**.** Let b be an integer.
Let $P(n)$ be a mathematical statement defined for each integer $n \geq b$.
Assume the following:

1. **Base case:** The statement $P(b)$ holds (i.e., the statement $P(n)$ holds when $n = b$).
2. **Induction step:** For each integer $n \geq b$, the implication $P(n) \implies P(n+1)$ holds.

Then, the statement $P(n)$ holds for every integer $n \geq b$.

We can restate this principle slightly by renaming the n in the induction step as $n-1$ (so that the implication $P(n) \implies P(n+1)$ turns into $P(n-1) \implies P(n)$). Thus it takes the following form:

Theorem 1.9.2 (Principle of Mathematical Induction, restated)**.** Let b be an integer.
Let $P(n)$ be a mathematical statement defined for each integer $n \geq b$.
Assume the following:

1. **Base case:** The statement $P(b)$ holds (i.e., the statement $P(n)$ holds when $n = b$).
2. **Induction step:** For each integer $n > b$, the implication $P(n-1) \implies P(n)$ holds.

Then, the statement $P(n)$ holds for every integer $n \geq b$.

The idea behind the principle (in either form) is that the base case gives us $P(b)$ whereas the induction step gives us the implications

$$\begin{aligned} P(b) &\implies P(b+1), \\ P(b+1) &\implies P(b+2), \\ P(b+2) &\implies P(b+3), \\ &\cdots \end{aligned}$$

which we can use to "escalate" from $P(b)$ to $P(n)$ for any $n \geq b$.

In the domino metaphor, the base case tips over the first domino, while the induction step ensures that each domino falls from the impact of the previous domino.

1.9.2. Strong induction

Now assume that the $(b+2)$-domino $P(b+2)$ falls not from the impact of the previous domino $P(b+1)$, but rather from the combined force of the dominos

$P(b)$ and $P(b+1)$. This would still suffice. In other words, instead of the implication

$$P(b+1) \implies P(b+2),$$

it suffices to have the weaker implication

$$(P(b) \text{ AND } P(b+1)) \implies P(b+2).$$

Likewise, we can replace the implication $P(b+2) \implies P(b+3)$ by the weaker implication

$$(P(b) \text{ AND } P(b+1) \text{ AND } P(b+2)) \implies P(b+3).$$

More generally, for each $n > b$, instead of proving the implication $P(n-1) \implies P(n)$, it will suffice to prove the weaker implication

$$(P(b) \text{ AND } P(b+1) \text{ AND } P(b+2) \text{ AND } \cdots \text{ AND } P(n-1)) \implies P(n)$$

(so the domino $P(n)$ is tipped over by the combined force of all the previously fallen dominos, not just by its one left neighbor).

This induction principle is called **strong induction**. Explicitly, it says the following:

Theorem 1.9.3 (Principle of Strong Induction)**.** Let b be an integer.
Let $P(n)$ be a mathematical statement defined for each integer $n \geq b$.
Assume the following:

1. **Base case:** The statement $P(b)$ holds (i.e., the statement $P(n)$ holds when $n = b$).
2. **Induction step:** For each integer $n > b$, the implication

   $$(P(b) \text{ AND } P(b+1) \text{ AND } P(b+2) \text{ AND } \cdots \text{ AND } P(n-1)) \implies P(n)$$

   holds.

Then, the statement $P(n)$ holds for every integer $n \geq b$.

Proofs using this principle are called **proofs by strong induction** or **strong induction proofs**. They differ from regular induction proofs as follows: In the induction step of a strong induction, you can use not only the previous statement $P(n-1)$, but also all the statements before it: $P(n-2)$ and $P(n-3)$ and so on all the way down to $P(b)$. So you can think of strong induction as "induction with a long memory".

1.9.3. Example: Proof of Binet's formula

Let us prove Binet's formula by strong induction:

Proof of Binet's formula. We strongly induct on n (i.e., we perform strong induction on n). That is, we let $P(n)$ denote the statement

$$\text{“}f_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}\text{”}$$

for each $n \geq 0$, and we apply the Principle of Strong Induction (for $b = 0$) to prove it.

Base case: As above, we check that Binet's formula holds for $n = 0$, i.e., that $P(0)$ is true.

Induction step: Let $n > 0$ be an integer. We must prove the implication

$$(P(0) \text{ AND } P(1) \text{ AND } P(2) \text{ AND } \cdots \text{ AND } P(n-1)) \Longrightarrow P(n).$$

Thus, we assume that $P(0)$ AND $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(n-1)$ holds. In other words, we assume that Binet's formula holds for 0, for 1, for 2, and so on, all the way up to $n-1$. Our goal is to prove $P(n)$, meaning that Binet's formula holds for n. In other words, our goal is to prove that $f_n = \dfrac{\varphi^n - \psi^n}{\sqrt{5}}$.

Now, we recall the definition of Fibonacci numbers:

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2} = \frac{\varphi^{n-1} - \psi^{n-1}}{\sqrt{5}} + \frac{\varphi^{n-2} - \psi^{n-2}}{\sqrt{5}} \\ &\qquad \left(\text{since } P(n-1) \text{ and } P(n-2) \text{ hold by assumption}\right) \\ &= \frac{1}{\sqrt{5}} \underbrace{\left(\varphi^{n-1} + \varphi^{n-2}\right)}_{\substack{=\varphi^{n-2}(\varphi+1) \\ =\varphi^{n-2}\varphi^2 \\ =\varphi^n \\ (\text{since } \varphi+1=\varphi^2)}} - \frac{1}{\sqrt{5}} \underbrace{\left(\psi^{n-1} + \psi^{n-2}\right)}_{\substack{=\psi^{n-2}(\psi+1) \\ =\psi^{n-2}\psi^2 \\ =\psi^n \\ (\text{since } \psi+1=\psi^2)}} \\ &= \frac{1}{\sqrt{5}}\varphi^n - \frac{1}{\sqrt{5}}\psi^n = \frac{\varphi^n - \psi^n}{\sqrt{5}}. \end{aligned}$$

So $P(n)$ is proved, and the induction step is complete, right?

.....

Almost. We have used $P(n-1)$ and $P(n-2)$, but our IH "only" said that $P(0)$ AND $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(n-1)$ holds. So the IH includes $P(n-1)$, but does it always include $P(n-2)$? Not when $n = 1$. So we need to handle the case $n = 1$ separately. But this is straightforward: If $n = 1$, then

$P(n)$ is saying that $f_1 = \dfrac{\varphi^1 - \psi^1}{\sqrt{5}}$, which can be easily checked:

$$\frac{\varphi^1 - \psi^1}{\sqrt{5}} = \frac{\varphi - \psi}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} = 1 = f_1.$$

Now we are done, because for any $n \geq 2$ we do know that both $P(n-1)$ and $P(n-2)$ are part of the IH $P(0)$ AND $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(n-1)$. □

So the above proof, in a sense, two de-facto bases cases:

1. the actual base case $n = 0$,
2. and the case $n = 1$, which is formally part of the induction step but had to be handled manually due to the IH being too weak in that case.

Proofs by strong induction often exhibit this behavior, particularly when the claim itself involves some sequence defined recursively with a dependence on the previous so-and-so-many values.

We will see more examples of strong induction proofs rather soon. First a remark:

Remark 1.9.4. In a strong induction proof – let's say with $b = 0$ – the base case is proving that $P(0)$ holds, whereas the induction step is proving that the implication

$$(P(0) \text{ AND } P(1) \text{ AND } P(2) \text{ AND } \cdots \text{ AND } P(n-1)) \Longrightarrow P(n)$$

holds, i.e., that $P(n)$ holds if we assume that all the previous P's hold. Thus, the base case is an instance of the same pattern as the induction step, just for $n = 0$, because in this case there are no previous P's, and so proving $P(n)$ assuming them is tantamount to just proving $P(0)$ unconditionally. In other words, we can "fold" the base case into the induction step when we are doing a strong induction. This is called **baseless strong induction**.

1.9.4. Example: Prime factorizations exist

Another example of a strong induction proof comes from elementary number theory. We recall two basic definitions (more on this later):

Definition 1.9.5. Let b be an integer. A **divisor** of b means an integer a satisfying $a \mid b$.

For example, the divisors of 6 are $1, 2, 3, 6, -1, -2, -3, -6$.

Definition 1.9.6. A **prime** (or **prime number**) means an integer $p > 1$ whose only positive divisors are 1 and p.

So the primes (in increasing order) are

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ \ldots.$$

There are infinitely many primes, as we will soon see.

Theorem 1.9.7. Every positive integer is a product of finitely many primes.

Here and in the following, an empty product (i.e., a product of no numbers) is understood to be 1. Thus, the theorem in particular holds for 1, since 1 is a product of finitely many primes (namely, of zero primes). Here are some more interesting examples:

- $2023 = 7 \cdot 17 \cdot 17$ is a product of three primes.
- $2024 = 2 \cdot 2 \cdot 2 \cdot 11 \cdot 23$ is a product of five primes.
- $2 = 2$ is a product of one prime.

Let us prove the theorem in general now:

Proof of the theorem. We must prove the statement

$$P(n) = (\text{“}n \text{ is a product of finitely many primes”})$$

for each integer $n \geq 1$.

We shall prove this by strong induction on n.

Base case: $P(1)$ is true, since 1 is a product of finitely many primes (namely, of no primes).

Induction step: Let $n > 1$. We must prove the implication

$$(P(1) \text{ AND } P(2) \text{ AND } \cdots \text{ AND } P(n-1)) \Longrightarrow P(n).$$

So we assume that $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(n-1)$ holds. We must prove that $P(n)$ holds.

In other words, we must prove that n is a product of finitely many primes.

We are in one of the following two cases:

Case 1: The only positive divisors of n are 1 and n.

Case 2: There is a positive divisor d of n that is neither 1 nor n.

Consider Case 1 first. In this case, n itself is prime, so that n is a product of one prime (itself), and we are done.

Now consider Case 2. In this case, there is a positive divisor d of n that is neither 1 nor n. Consider this d. Easily, $1 < d < n$ (see later for the proper justification here; essentially, a divisor cannot be larger than what it divides).

Furthermore, $\frac{n}{d}$ is an integer (since d is a divisor of n), and also satisfies $1 < \frac{n}{d} < n$ (indeed, this is just $1 < d < n$ after some equivalence transformations).

Our IH says that $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(n-1)$ holds. In other words, $P(k)$ holds for every positive integer $k < n$. In other words, each positive integer $k < n$ is a product of finitely many primes. Hence, in particular, d and $\frac{n}{d}$ are such products:

$$d = p_1 p_2 \cdots p_k \qquad \text{and} \qquad \frac{n}{d} = q_1 q_2 \cdots q_\ell,$$

where all the p_i's and all the q_j's are primes. Now,

$$n = \frac{n}{d} \cdot d = q_1 q_2 \cdots q_\ell \cdot p_1 p_2 \cdots p_k,$$

and this shows that n is a product of finitely many primes. In other words, $P(n)$ holds, and the induction step is complete, so we are done. □

1.9.5. Example: Paying with 3-cent and 5-cent coins

Here is another example of strong induction:

Exercise 1.9.1. Assume that you have 3-cent coins and 5-cent coins (each in infinite supply). What denominations can you pay with these coins?

Let's make a table:

0 cents	yes
1 cent	no
2 cents	no
3 cents	yes
4 cents	no
5 cents	yes
6 cents	yes: $2 \cdot 3$
7 cents	no
8 cents	yes: $3 + 5$
9 cents	yes: $3 \cdot 3$
10 cents	yes: $2 \cdot 5$
11 cents	yes: $2 \cdot 3 + 5$
12 cents	yes: $4 \cdot 3$
13 cents	yes: $2 \cdot 5 + 3$
$\vdots$	$\vdots$

Experimentally, it looks like all denominations ≥ 8 cents can be paid. Why?

We can notice that every denomination divisible by 3 cents can be paid. Moreover, if a denomination k (that is, k cents) can be paid, then so can $k+3$ (just add another 3-cent coin). Thus, because we can pay 8 cents, we can also pay $11, 14, 17, \ldots$ cents. Because we can pay 9 cents, we can likewise pay $12, 15, 18, \ldots$ cents. Finally, because we can pay 10 cents, we can likewise pay $13, 16, 19, \ldots$ cents. These three sequences together cover all integers ≥ 8, so we can indeed pay any (integer) denomination ≥ 8 cents.

Let us formalize this as a strong induction proof.

We define $\mathbb{N}$ to be the set of all nonnegative integers:

$$\mathbb{N} = \{0, 1, 2, \ldots\}.$$

Proposition 1.9.8. For any integer $n \geq 8$, we can pay n cents with 3-cent and 5-cent coins. In other words, any integer $n \geq 8$ can be written as $n = 3a + 5b$ with $a, b \in \mathbb{N}$.

Proof. We proceed by strong induction on n:

Base case: For $n = 8$, the claim is true, since $8 = 3 \cdot 1 + 5 \cdot 1$.

Induction step: Fix an integer $n > 8$. Assume that the proposition is already proved for all the integers $8, 9, \ldots, n-1$. We must prove that it is also true for n. In other words, we must prove that we can pay n cents with 3-cent and 5-cent coins.

We are in one of the following three cases (since $n > 8$):

Case 1: We have $n = 9$.

Case 2: We have $n = 10$.

Case 3: We have $n \geq 11$.

In Case 1, we are done since $n = 9 = 3 \cdot 3 + 5 \cdot 0$.

In Case 2, we are done since $n = 10 = 3 \cdot 0 + 5 \cdot 2$.

Now consider Case 3. In this case, $n \geq 11$, so that $n - 3 \geq 8$. Therefore we can apply our IH to see that the proposition is true for $n - 3$ instead of n. So we see that $n - 3$ can be paid with 3-cent and 5-cent coins:

$$n - 3 = 3c + 5d \qquad \text{for some } c, d \in \mathbb{N}.$$

Thus,

$$n = 3 + 3c + 5d = 3(c + 1) + 5d,$$

so that n cents can also be paid with 3-cent and 5-cent coins. This completes the induction step, qed (= what we desired to prove = our proof is finished). □

Note that the above proof had one "de-jure base case" (the case $n = 8$), but also two "de-facto base cases" (the cases $n = 9$ and $n = 10$), which had to be handled separately even though they were part of the induction step. We could just as well have used baseless strong induction, in which case $n = 8$ would also be a de-facto base case. Alternatively, we could have declared them all to be base cases.

2. Sums and products

2.1. Finite sums

We have already encountered sums such as

$$x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + x^2y^{n-3} + xy^{n-2} + y^{n-1}.$$

Sums like this can be tricky to decipher, since you have to figure out what the "$\cdots$" means. As sums get more complicated, this gets harder and more error-prone. So we need a rigorous and short notation for sums like this. This is the **finite sum notation** aka the **sigma notation**. In its simplest form, it is defined as follows:

Definition 2.1.1. Let u and v be two integers. Let $a_u, a_{u+1}, \ldots, a_v$ be some numbers. Then,

$$\sum_{k=u}^{v} a_k$$

is defined to be the sum

$$a_u + a_{u+1} + \cdots + a_v$$

(in more detail: $a_u + a_{u+1} + a_{u+2} + \cdots + a_{v-1} + a_v$). It is called the **sum of the numbers a_k where k ranges from u to v**. When $v < u$, this sum is called **empty** and defined to be 0.

For instance,

$$\sum_{k=5}^{10} k = 5+6+7+8+9+10 = 45;$$

$$\sum_{k=5}^{10} \frac{1}{k} = \frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\frac{1}{9}+\frac{1}{10} = \frac{2131}{2520};$$

$$\sum_{k=5}^{10} k^k = 5^5+6^6+7^7+8^8+9^9+10^{10};$$

$$\sum_{k=5}^{5} k = 5;$$

$$\sum_{k=5}^{4} k = 0 \qquad \text{(an empty sum)};$$

$$\sum_{k=5}^{3} k = 0 \qquad \text{(an empty sum)};$$

$$\sum_{k=5}^{8} 3 = 3+3+3+3 = 4\cdot 3 = 12;$$

$$\sum_{k=0}^{n-1} q^k = q^0+q^1+\cdots+q^{n-1};$$

$$\begin{aligned}\sum_{k=0}^{n-1} x^k y^{n-1-k} &= x^0y^{n-1}+x^1y^{n-2}+x^2y^{n-3}+\cdots+x^{n-3}y^2+x^{n-2}y^1+x^{n-1}y^0 \\ &= y^{n-1}+xy^{n-2}+x^2y^{n-3}+\cdots+x^{n-3}y^2+x^{n-2}y+x^{n-1} \\ &= x^{n-1}+x^{n-2}y+x^{n-3}y^2+\cdots+x^2y^{n-3}+xy^{n-2}+y^{n-1}.\end{aligned}$$

Thus, one of our above theorems, which stated that

$$(x-y)\left(x^{n-1}+x^{n-2}y+x^{n-3}y^2+\cdots+x^2y^{n-3}+xy^{n-2}+y^{n-1}\right) = x^n-y^n$$

holds, can now be restated as

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

The variable k is not set in stone; you can replace it by any other variable that is not already occupied with a different meaning. For example,

$$\sum_{k=u}^{v} a_k = \sum_{\ell=u}^{v} a_\ell = \sum_{\spadesuit=u}^{v} a_\spadesuit.$$

Just don't make it $\sum_{u=u}^{v} a_u$.

Here are some more examples: For any $n \in \mathbb{N}$, we have

$$\sum_{k=1}^{n} k = 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \qquad \text{(by Little Gauss)};$$

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

$$\sum_{k=1}^{n} 1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ ones}} = n \cdot 1 = n;$$

$$\sum_{k=1}^{n} (2k-1) = 1 + 3 + 5 + \cdots + (2n-1).$$

Let us actually compute this last sum. I will use the following two laws of summation:

- We have
$$\sum_{k=u}^{v} (a_k - b_k) = \sum_{k=u}^{v} a_k - \sum_{k=u}^{v} b_k$$
for any integers u, v and any numbers a_k, b_k.
- We have
$$\sum_{k=u}^{v} \lambda a_k = \lambda \sum_{k=u}^{v} a_k$$
for any integers u, v and any numbers λ and a_k.

Rules like this are dime a dozen; I give a reference to a list, but you should be able to come up with them on your own. Let us now compute our sum:

$$\begin{aligned}
\sum_{k=1}^{n} (2k-1) &= \underbrace{\sum_{k=1}^{n} 2k}_{=2\sum_{k=1}^{n} k} - \underbrace{\sum_{k=1}^{n} 1}_{=n} \\
&= 2 \underbrace{\sum_{k=1}^{n} k}_{=\frac{n(n+1)}{2}} - n = 2 \cdot \frac{n(n+1)}{2} - n \\
&= n(n+1) - n = n^2.
\end{aligned}$$

For another illustration of how summation signs are used, let me rewrite Gauss's proof of the Little Gauss formula

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

using this notation. We will need three new rules for this:

- We have
$$\sum_{k=u}^{v} a_k + \sum_{k=u}^{v} b_k = \sum_{k=u}^{v} (a_k + b_k) .$$
- We have
$$\sum_{k=u}^{v} a_k = \sum_{k=u}^{v} a_{u+v-k}.$$
Written out explicitly, this is saying that
$$\begin{aligned} &a_u + a_{u+1} + \cdots + a_{v-1} + a_v \\ &= a_v + a_{v-1} + \cdots + a_{u+1} + a_u. \end{aligned}$$
In other words, this is just saying that the sum of a bunch of numbers does not change if we reverse the order of these numbers.
- For any integers $u \leq v$ and any number λ, we have
$$\sum_{k=u}^{v} \lambda = (v - u + 1)\, \lambda.$$
Don't forget the $+1$.

Now, Gauss's proof takes the following shape:
$$2\sum_{k=1}^{n} k = \sum_{k=1}^{n} k + \underbrace{\sum_{k=1}^{n} k}_{\substack{=\sum_{k=1}^{n} (n+1-k) \\ \text{(by reversing the order)}}} = \sum_{k=1}^{n} k + \sum_{k=1}^{n} (n+1-k)$$
$$= \sum_{k=1}^{n} \underbrace{(k + (n+1-k))}_{=n+1} = \sum_{k=1}^{n} (n+1) = n \cdot (n+1) ,$$
so that $\sum\limits_{k=1}^{n} k = \dfrac{n \cdot (n+1)}{2}$.

We have now seen closed-form expressions (i.e., expressions without Σ signs or "$\cdots$"s) for several sums. Not every sum has such an expression. For instance, neither $\sum\limits_{k=1}^{n} \dfrac{1}{k}$ nor $\sum\limits_{k=1}^{n} k^k$ has a closed-form expression.

Some more terminology:

The notation $\sum\limits_{k=u}^{v} a_k$ is called **sigma notation** or **finite sum notation**. The symbol $\sum$ itself is called the **summation sign**. The variables u and v are called the **lower limit** and the **upper limit** of the summation. The variable k is called the **summation index** or the **running index**, and is said to **range** (or **run**) from u to v. The numbers a_k are called the **addends** of the finite sum.

We note two more rules for finite sums:

- The "splitting-off" rule: For any integer $u \leq v$ and any numbers $a_u, a_{u+1}, \ldots, a_v$, we have
$$\sum_{k=u}^{v} a_k = a_u + \sum_{k=u+1}^{v} a_k = \sum_{k=u}^{v-1} a_k + a_v.$$
In other words, we can compute a sum by splitting it into its first or last addend and the rest of the sum.
- More generally, any finite sum $\sum_{k=u}^{v} a_k$ can be split at any point: We have
$$\sum_{k=u}^{v} a_k = \sum_{k=u}^{w} a_k + \sum_{k=w+1}^{v} a_k$$
for any integers $u \leq w \leq v$ (actually, even more generally, for $u-1 \leq w \leq v$).

Finite sum notation, in the form defined above, is helpful when the summation index is running over an integer interval (i.e., all integers from u to v for certain u and v). But sometimes, you want the range to be something else, such as "all the even numbers between 0 and 16". In this case, you can use slightly modified versions of finite sum notation: e.g.,
$$\sum_{k \in \{1,2,\ldots,n\} \text{ is even}} k = 2 + 4 + 6 + \cdots + m,$$
where m is the largest even element of $\{1, 2, \ldots, n\}$. We won't use this much, but this notation is rather self-explanatory.

2.2. Finite products

Finite products are just like finite sums, but you are multiplying instead of adding. The notation for them is $\prod_{k=u}^{v} a_k$. An empty product is defined to be 1. Here are the details:

Definition 2.2.1. Let u and v be two integers. Let $a_u, a_{u+1}, \ldots, a_v$ be some numbers. Then,
$$\prod_{k=u}^{v} a_k$$
is defined to be the product
$$a_u a_{u+1} \cdots a_v$$
(in more detail: $a_u a_{u+1} a_{u+2} \cdots a_{v-1} a_v$). It is called the **product of the numbers** a_k **where** k **ranges from** u **to** v. When $v < u$, this product is called **empty** and defined to be 1.

For example:

$$\prod_{k=5}^{10} k = 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10;$$

$$\prod_{k=5}^{10} \frac{1}{k} = \frac{1}{5} \cdot \frac{1}{6} \cdot \frac{1}{7} \cdot \frac{1}{8} \cdot \frac{1}{9} \cdot \frac{1}{10};$$

$$\prod_{k=5}^{5} \frac{1}{k} = \frac{1}{5};$$

$$\prod_{k=6}^{5} \frac{1}{k} = 1 \qquad \text{(an empty product)};$$

$$\prod_{k=1}^{n} a = \underbrace{aa \cdots a}_{n \text{ times}} = a^n;$$

$$\prod_{k=1}^{n} a^k = a^1 a^2 \cdots a^n = a^{1+2+\cdots+n}$$

$$\left(\begin{array}{c} \text{by one of the laws of exponents:} \\ a^{i_1} a^{i_2} \cdots a^{i_k} = a^{i_1+i_2+\cdots+i_k} \end{array} \right)$$

$$= a^{n(n+1)/2} \qquad \text{by Little Gauss.}$$

The notation $\prod_{k=u}^{v} a_k$ is called **finite product notation**. The symbol $\prod$ itself is called the **product sign**. The variables u and v are called the **lower limit** and the **upper limit** of the product. The variable k is called the **product index** or the **running index**, and is said to **range** (or **run**) from u to v. The numbers a_k are called the **factors** of the finite sum.

Lots of properties of finite sums have analogues for finite products. For example:

- The "splitting-off" rule: For any integer $u \leq v$ and any numbers $a_u, a_{u+1}, \ldots, a_v$, we have
$$\prod_{k=u}^{v} a_k = a_u \cdot \prod_{k=u+1}^{v} a_k = \left(\prod_{k=u}^{v-1} a_k \right) \cdot a_v.$$
In other words, we can compute a product by splitting it into its first or last factor and the rest of the product.

- More generally, any finite product $\prod_{k=u}^{v} a_k$ can be split at any point: We have
$$\prod_{k=u}^{v} a_k = \left(\prod_{k=u}^{w} a_k \right) \left(\prod_{k=w+1}^{v} a_k \right)$$

for any integers $u \leq w \leq v$ (actually, even more generally, for $u - 1 \leq w \leq v$).

2.3. Factorials

Now we define a sequence of integers that appears all across mathematics. Recall the notation $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Definition 2.3.1. For any $n \in \mathbb{N}$, we define the positive integer $n!$ (called the **factorial** of n, and often pronounced "n **factorial**") by

$$n! = \prod_{k=1}^{n} k = 1 \cdot 2 \cdot \cdots \cdot n.$$

This is the product of the first n positive integers.

For example,

$$\begin{aligned}
0! &= (\text{empty product}) = 1; \\
1! &= 1; \\
2! &= 1 \cdot 2 = 2; \\
3! &= 1 \cdot 2 \cdot 3 = 6; \\
4! &= 1 \cdot 2 \cdot 3 \cdot 4 = 24; \\
5! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120; \\
6! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720; \\
7! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 5\,040; \\
8! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 = 40\,320; \\
9! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 = 362\,880; \\
10! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 3\,628\,800.
\end{aligned}$$

Proposition 2.3.2 (recursion of the factorials)**.** For every positive integer n, we have

$$n! = (n-1)! \cdot n.$$

Proof. Let n be a positive integer. Then,

$$n! = 1 \cdot 2 \cdot \cdots \cdot n = \underbrace{(1 \cdot 2 \cdot \cdots \cdot (n-1))}_{=(n-1)!} \cdot n = (n-1)! \cdot n.$$

□

2.4. Binomial coefficients: definition

We shall next define one of the most important families of numbers in mathematics:

Definition 2.4.1. Let n and k be any numbers. Then, we define a number $\binom{n}{k}$ as follows:

- If $k \in \mathbb{N}$, then we set

$$\binom{n}{k} := \frac{n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right)}{k!}.$$

  (The numerator is a product of k factors, starting at n and going down by 1 at every step. You can write this product as $\prod_{i=0}^{k-1}\left(n-i\right)$.)

- If $k \notin \mathbb{N}$, then we set

$$\binom{n}{k} := 0.$$

The number $\binom{n}{k}$ (do not mistake it for a vector $\begin{pmatrix} n \\ k \end{pmatrix}$) is called "$n$ **choose** k", and is known as the **binomial coefficient** of n and k.

Example 2.4.2. For any number n, we have

$$\begin{aligned}
\binom{n}{3} &= \frac{n\left(n-1\right)\left(n-2\right)}{3!} = \frac{n\left(n-1\right)\left(n-2\right)}{6}; \\
\binom{n}{2} &= \frac{n\left(n-1\right)}{2!} = \frac{n\left(n-1\right)}{2}; \\
\binom{n}{1} &= \frac{n}{1!} = n; \\
\binom{n}{0} &= \frac{\left(\text{empty product}\right)}{0!} = \frac{1}{1} = 1; \\
\binom{n}{-1} &= 0 \qquad \left(\text{since } -1 \notin \mathbb{N}\right); \\
\binom{n}{2.5} &= 0 \qquad \left(\text{since } 0.5 \notin \mathbb{N}\right).
\end{aligned}$$

For any $k \in \mathbb{N}$, we have

$$\binom{0}{k} = \frac{0\,(0-1)\,(0-2)\cdots(0-k+1)}{k!} = \begin{cases} 0, & \text{if } k > 0; \\ 1, & \text{if } k = 0; \end{cases}$$

$$\begin{aligned}\binom{-1}{k} &= \frac{(-1)\,(-1-1)\,(-1-2)\cdots(-1-k+1)}{k!} \\ &= \frac{(-1)\,(-2)\,(-3)\cdots(-k)}{k!} = (-1)^k \underbrace{\frac{1\cdot 2\cdot 3\cdot\cdots\cdot k}{k!}}_{=1} \\ &= (-1)^k.\end{aligned}$$

Let us tabulate the values of $\binom{n}{k}$ for $n, k \in \mathbb{N}$:

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$
$n=0$	1	0	0	0	0	0	0
$n=1$	1	1	0	0	0	0	0
$n=2$	1	2	1	0	0	0	0
$n=3$	1	3	3	1	0	0	0
$n=4$	1	4	6	4	1	0	0
$n=5$	1	5	10	10	5	1	0
$n=6$	1	6	15	20	15	6	1

Proposition 2.4.3. Let $n \in \mathbb{N}$ and $k > n$. Then, $\binom{n}{k} = 0$.

Proof. If $k \notin \mathbb{N}$, then this is clear by definition. Otherwise, again by definition,

$$\binom{n}{k} = \frac{n\,(n-1)\,(n-2)\cdots(n-k+1)}{k!} = \frac{0}{k!},$$

since one of the factors in the product $n\,(n-1)\,(n-2)\cdots(n-k+1)$ is 0). For instance, for $n = 3$ and $k = 6$, we have

$$\binom{3}{6} = \frac{3\cdot 2\cdot 1\cdot 0\cdot(-1)\cdot(-2)}{6!} = \frac{0}{6!}.$$

□

Proposition 2.4.4. Let $n \in \mathbb{N}$. Then, $\binom{n}{n} = 1$.

Proof. We have

$$\binom{n}{n} = \frac{n\,(n-1)\,(n-2)\cdots(n-n+1)}{n!} = \frac{n\,(n-1)\,(n-2)\cdots 1}{n!} = 1$$

(since $n\,(n-1)\,(n-2)\cdots 1 = 1\cdot 2\cdot 3\cdot\cdots\cdot n = n!$). □

Remark 2.4.5. Neither of the two above propositions would work if we dropped the $n \in \mathbb{N}$ requirements. For instance, $\binom{2.5}{4} = \frac{2.5 \cdot 1.5 \cdot 0.5 \cdot (-0.5)}{4!} \neq 0$ and $\binom{2.5}{2.5} = 0 \neq 1$.

The first proposition above says that the numbers $\binom{n}{k}$ for $n, k \in \mathbb{N}$ are only interesting in the $k \leq n$ region. This suggests drawing the table of those "interesting" $\binom{n}{k}$ in a slanted way, where the n corresponds to the row and the k corresponds to the diagonal.

													$k{=}0$ ↙													
$n=0$	$\to$											1		$k{=}1$ ↙												
$n=1$	$\to$									1		1			$k{=}2$ ↙											
$n=2$	$\to$							1		2		1				$k{=}3$ ↙										
$n=3$	$\to$						1		3		3		1				$k{=}4$ ↙									
$n=4$	$\to$					1		4		6		4		1				$k{=}5$ ↙								
$n=5$	$\to$				1		5		10		10		5		1				$k{=}6$ ↙							
$n=6$	$\to$			1		6		15		20		15		6		1				$k{=}7$ ↙						
$n=7$	$\to$		1		7		21		35		35		21		7		1									
$n=8$	$\to$	1		8		28		56		70		56		28		8		1								

Staring for long enough at this triangle reveals a few more properties:

√ **Pascal's identity, aka the recurrence of the binomial coefficients:** For any numbers n and k, we have

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

- **Integrality of binomial coefficients:** For any $n \in \mathbb{Z}$ and any k, we have $\binom{n}{k} \in \mathbb{Z}$.

√ **Symmetry:** For any $n \in \mathbb{N}$ and k, we have

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

We will prove these in the next section.

2.5. Binomial coefficients: properties

2.5.1. Pascal's identity

We begin with the most important fact about binomial coefficients:

Theorem 2.5.1 (Pascal's identity, aka the recurrence of the binomial coefficients)**.** For any numbers n and k, we have

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

Example 2.5.2. For $n = 7$ and $k = 3$, this says that

$$\underbrace{\binom{7}{3}}_{=35} = \underbrace{\binom{6}{2}}_{=15} + \underbrace{\binom{6}{3}}_{=20}.$$

Proof of Pascal's identity. Let n and k be two numbers. We are in one of the following three cases:

Case 1: The number k is a positive integer.

Case 2: We have $k = 0$.

Case 3: None of the above.

Let us first consider Case 1. In this case, k is a positive integer, so that both k and $k-1$ belong to $\mathbb{N}$. Thus, by the definition of BCs (= binomial coefficients), we have

$$\begin{aligned}
\binom{n}{k} &= \frac{n\,(n-1)\,(n-2)\cdots(n-k+1)}{k!}; \\
\binom{n-1}{k-1} &= \frac{(n-1)\,((n-1)-1)\,((n-1)-2)\cdots((n-1)-(k-1)+1)}{(k-1)!} \\
&= \frac{(n-1)\,(n-2)\,(n-3)\cdots(n-k+1)}{(k-1)!}; \\
\binom{n-1}{k} &= \frac{(n-1)\,(n-2)\,(n-3)\cdots((n-1)-k+1)}{k!} \\
&= \frac{(n-1)\,(n-2)\,(n-3)\cdots(n-k)}{k!}.
\end{aligned}$$

We let

$$a := (n-1)\,(n-2)\,(n-3)\cdots(n-k+1)\,;$$

this is the common factor in all three numerators. So the above formulas become

$$\binom{n}{k} = \frac{na}{k!}; \qquad \binom{n-1}{k-1} = \frac{a}{(k-1)!}; \qquad \binom{n-1}{k} = \frac{a\,(n-k)}{k!}.$$

So what we must prove can be rewritten as

$$\frac{na}{k!} = \frac{a}{(k-1)!} + \frac{a\,(n-k)}{k!}.$$

Rewriting $k!$ as $(k-1)! \cdot k$ (by the recursion of the factorials), this becomes

$$\frac{na}{(k-1)! \cdot k} = \frac{a}{(k-1)!} + \frac{a\,(n-k)}{(k-1)! \cdot k}.$$

Cancelling the common factor $\dfrac{a}{(k-1)!}$ turns this into

$$\frac{n}{k} = 1 + \frac{n-k}{k},$$

which is easily seen to hold. So the theorem is proved in Case 1.

Now consider Case 2. In this case, $k = 0$, so we must prove that

$$\underbrace{\binom{n}{0}}_{=1} = \underbrace{\binom{n-1}{-1}}_{=0} + \underbrace{\binom{n-1}{0}}_{=1},$$

which is true.

Finally, consider Case 3. In this case, $k \notin \mathbb{N}$, so that $k-1 \notin \mathbb{N}$. Hence, we must prove that

$$\underbrace{\binom{n}{k}}_{=0} = \underbrace{\binom{n-1}{k-1}}_{=0} + \underbrace{\binom{n-1}{k}}_{=0},$$

which is true.

So the theorem is proved in all three cases. □

2.5.2. The factorial formula

Binomial coefficients $\dbinom{n}{k}$ make sense for arbitrary n and k. However, when n and k are nonnegative integers with $k \leq n$, there is a particularly simple formula for $\dbinom{n}{k}$, known as the **factorial formula**:

Theorem 2.5.3 (factorial formula)**.** Let $n \in \mathbb{N}$ and $k \in \{0, 1, \ldots, n\}$. Then,

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

Proof. The definition of $\binom{n}{k}$ yields

$$\binom{n}{k} = \frac{n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right)}{k!}.$$

But

$$\begin{aligned}
&n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right) \\
&= \frac{n\left(n-1\right)\left(n-2\right)\cdots 1}{\left(n-k\right)\left(n-k-1\right)\cdots 1} \qquad \left(\begin{array}{c}\text{here we multiplied the product by the} \\ \text{extra factors } n-k,\ n-k-1,\ \ldots,\ 1, \\ \text{and then divided them back out}\end{array}\right) \\
&= \frac{1\cdot 2\cdot\cdots\cdot n}{1\cdot 2\cdot\cdots\cdot\left(n-k\right)} = \frac{n!}{\left(n-k\right)!},
\end{aligned}$$

so this becomes

$$\binom{n}{k} = \frac{\left(\dfrac{n!}{\left(n-k\right)!}\right)}{k!} = \frac{n!}{k!\cdot\left(n-k\right)!}.$$

□

Keep in mind that the factorial formula

$$\binom{n}{k} = \frac{n!}{k!\cdot\left(n-k\right)!}$$

would make no sense if we applied it to $n = \sqrt{2}$ or $k = -2$ or $k > n$. So its range of applicability is much smaller than that of the definition. This is why we didn't pick it as the definition!

2.5.3. The symmetry of binomial coefficients

Theorem 2.5.4 (symmetry of binomial coefficients)**.** For any $n \in \mathbb{N}$ and any number k, we have

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

Proof. We are in one of the following four cases:
Case 1: We have $k \in \{0, 1, \ldots, n\}$.
Case 2: We have $k < 0$.
Case 3: We have $k > n$.
Case 4: The number k is not an integer.
In Case 4, we are just claiming $0 = 0$, which is obvious.

In Case 1, we can apply the factorial formula to get

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} \qquad \text{and}$$
$$\binom{n}{n-k} = \frac{n!}{(n-k)! \cdot (n-(n-k))!} = \frac{n!}{(n-k)! \cdot k!} = \frac{n!}{k! \cdot (n-k)!}.$$

Clearly, these are equal.

It remains to deal with Cases 2 and 3. Both are easy (again you have to show that $0 = 0$). See the notes for details. □

Warning 2.5.5. The symmetry theorem holds only for $n \in \mathbb{N}$. For $n = -1$ and $k = 0$, it is false, since $\binom{-1}{0} = 1$ but $\binom{-1}{-1} = 0$.

2.5.4. Upper negation

Theorem 2.5.6 (Upper negation)**.** For any number n and any integer k, we have

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

Proof. If $k \notin \mathbb{N}$, then this is just saying $0 = (-1)^k \cdot 0$, which is clear.

If $k \in \mathbb{N}$, then we use the definition of BCs to see that

$$\begin{aligned}\binom{-n}{k} &= \frac{(-n)(-n-1)(-n-2)\cdots(-n-k+1)}{k!} \\ &= (-1)^k \cdot \frac{n(n+1)(n+2)\cdots(n+k-1)}{k!} \qquad \text{and} \\ \binom{n+k-1}{k} &= \frac{(n+k-1)(n+k-2)(n+k-3)\cdots n}{k!} \\ &= \frac{n(n+1)(n+2)\cdots(n+k-1)}{k!}.\end{aligned}$$

Compare and conclude. □

The upper negation theorem explains why there is an invisible copy of Pascal's triangle above the actual Pascal's triangle (in rows $-1, -2, -3, \ldots$).

2.5.5. Integrality of binomial coefficients

Theorem 2.5.7. For any $n \in \mathbb{N}$ and any number k, we have $\binom{n}{k} \in \mathbb{N}$.

Proof. We induct on n.

Base case: The theorem holds for $n = 0$, since any number k satisfies

$$\binom{0}{k} = \begin{cases} 1, & \text{if } k = 0; \\ 0, & \text{if } k \neq 0 \end{cases} \qquad \text{(easy to see from the definition)}$$
$$\in \mathbb{N}.$$

Induction step: We make a step from $n-1$ to n. So we fix a positive integer n, and we assume (as the IH) that the theorem holds for $n-1$. In other words, we assume that

$$\binom{n-1}{k} \in \mathbb{N} \qquad \text{for all numbers } k.$$

Now we must prove that the theorem holds for n, i.e., that

$$\binom{n}{k} \in \mathbb{N} \qquad \text{for all numbers } k.$$

But this is easy: Pascal's identity yields

$$\binom{n}{k} = \underbrace{\binom{n-1}{k-1}}_{\substack{\in\mathbb{N} \\ \text{(by the IH,} \\ \text{applied to } k-1 \\ \text{instead of } k)}} + \underbrace{\binom{n-1}{k}}_{\substack{\in\mathbb{N} \\ \text{(by the IH)}}} \in \mathbb{N}.$$

Thus the induction step is complete, and the theorem proved. □

Corollary 2.5.8. For any $n \in \mathbb{Z}$ and any number k, we have $\binom{n}{k} \in \mathbb{Z}$.

Proof. If $n \in \mathbb{N}$, then this follows from the previous theorem.

So remains to handle case when $n \notin \mathbb{N}$. In this case, $n \in \{-1, -2, -3, \ldots\}$, so that $n \leq -1$ and therefore $-n \geq 1$.

We assume that $k \in \mathbb{N}$, since otherwise $\binom{n}{k} = 0 \in \mathbb{Z}$. Hence, $k \geq 0$. Thus, $\underbrace{-n}_{\geq 1} + \underbrace{k}_{\geq 0} - 1 \geq 1 + 0 - 1 = 0$. In other words, $-n + k - 1 \in \mathbb{N}$.

Now, the upper negation formula (applied to $-n$ instead of n) yields

$$\binom{-(-n)}{k} = (-1)^k \underbrace{\binom{-n+k-1}{k}}_{\substack{\in\mathbb{N} \\ \text{(by the theorem above,} \\ \text{since } -n+k-1 \in \mathbb{N})}} \in \mathbb{Z}.$$

So we are done in this case, too, and the corollary is proved. □

2.5.6. Finding Fibonacci in Pascal's triangles

The binomial coefficients are related to the Fibonacci numbers:

Theorem 2.5.9. For any $n \in \mathbb{N}$, the Fibonacci number f_{n+1} is

$$\begin{aligned} f_{n+1} &= \binom{n-0}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots + \binom{n-n}{n} \\ &= \sum_{i=0}^{n} \binom{n-i}{i}. \end{aligned}$$

We could prove this by strong induction on n, but we will later see a more conceptual proof of this, so we skip the induction proof.

2.6. Why "n choose k"?

We have proved that $\binom{n}{k} \in \mathbb{N}$ whenever $n \in \mathbb{N}$ by inducting on n. But there is a more conceptual explanation of the same result, which proceeds by answering the question "what does $\binom{n}{k}$ count?". Namely, $\binom{n}{k}$ counts the k-element subsets of a given n-element set, i.e., the ways to choose k out of n objects if the order doesn't matter and we choose without replacement (i.e., we cannot choose the same object twice). In more rigorous terms:

Theorem 2.6.1 (combinatorial interpretation of binomial coefficients)**.** Let $n \in \mathbb{N}$ and let k be any number. Let A be any n-element set (i.e., a set that has exactly n distinct elements). Then,

$$\binom{n}{k} \text{ is the number of } k\text{-element subsets of } A.$$

Example 2.6.2. Let $n = 4$ and $k = 2$ and $A = \{1,2,3,4\}$. Then, the 2-element subsets of A are

$$\{1,2\}, \quad \{1,3\}, \quad \{1,4\}, \quad \{2,3\}, \quad \{2,4\}, \quad \{3,4\}$$

(note that we are not listing $\{2,1\}$ extra, since it is the same subset as $\{1,2\}$; also note that $\{1,1\}$ is not allowed, since it is a 1-element subset: $\{1,1\} = \{1\}$). So the number of these 2-element subsets is 6. The theorem above says that this number is $\binom{n}{k} = \binom{4}{2} = \frac{4 \cdot 3}{2!} = 6$.

We won't prove the theorem right now, since it would require us to be precise about what "the number of [some things]" means, and there will be an entire chapter devoted to that.

Note that the theorem does not say anything about $\binom{-3}{5}$.

2.7. The binomial formula

The reason why binomial coefficients got their name is the **binomial formula**:

Theorem 2.7.1 (binomial formula, aka binomial theorem)**.** Let a and b be two numbers, and let $n \in \mathbb{N}$. Then,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}. \tag{BF1}$$

Restated without the summation sign:

$$(a+b)^n = \underbrace{\binom{n}{0} a^0 b^{n-0}}_{=b^n} + \underbrace{\binom{n}{1} a^1 b^{n-1}}_{=nab^{n-1}} + \cdots + \underbrace{\binom{n}{n} a^n b^{n-n}}_{=a^n}.$$

Equivalently,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k. \tag{BF2}$$

Proof. The formula (BF2) is just the formula (BF1) with the variables a and b swapped. (Or you can write the sum upside-down and use the symmetry of BCs.) Thus it suffices to prove one of the two formulas. Let us prove (BF1).

We proceed by induction on n:

Base case: For $n = 0$, the formula (BF1) is saying

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

The LHS is 1, whereas the RHS is $\underbrace{\binom{0}{0}}_{=1} \underbrace{a^0}_{=1} \underbrace{b^{0-0}}_{=1} = 1$. So the formula is true for $n = 0$.

Induction step: Let $n \in \mathbb{N}$. Assume (as the IH) that (BF1) holds for n. In other words, assume that

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

We must show that (BF1) also holds for $n+1$. In other words, we must show that

$$(a+b)^{n+1} \stackrel{?}{=} \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.$$

Indeed, we have

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)^n \cdot (a+b) \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right) \cdot (a+b) \qquad \text{(by the IH)} \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right) \cdot a + \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right) \cdot b \\
&= \sum_{k=0}^{n} \binom{n}{k} \underbrace{a^k b^{n-k} a}_{=a^{k+1} b^{n-k}} + \sum_{k=0}^{n} \binom{n}{k} a^k \underbrace{b^{n-k} b}_{\substack{=b^{n-k+1} \\ =b^{n+1-k}}} \\
&\qquad\qquad \left(\begin{array}{c} \text{by distributivity for finite sums, i.e., by} \\ \text{the rule } \left(\sum_{s=u}^{v} a_s \right) c = \sum_{s=u}^{v} a_s c \end{array} \right) \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k}.
\end{aligned}$$

On the other hand,

$$\begin{aligned}
&\sum_{k=0}^{n+1} \underbrace{\binom{n+1}{k}}_{\substack{= \binom{n}{k-1} + \binom{n}{k} \\ \text{(by the recurrence of the BCs,} \\ \text{aka Pascal's identity)}}} a^k b^{n+1-k} \\
&= \sum_{k=0}^{n+1} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} \\
&= \sum_{k=0}^{n+1} \left(\binom{n}{k-1} a^k b^{n+1-k} + \binom{n}{k} a^k b^{n+1-k} \right) \\
&= \sum_{k=0}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n+1-k}
\end{aligned}$$

(by the summation rule $\sum (c_s + d_s) = \sum c_s + \sum d_s$).

So we have now shown the two equalities

$$(a+b)^{n+1} = \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \qquad \text{and}$$
$$\sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k} = \sum_{k=0}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n+1-k}.$$

Our goal is to show that the LHSs of these two equalities are equal. We can just as well show that their RHSs are equal (since LHS = RHS). In other words, we can just as well show that

$$\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k}$$
$$= \sum_{k=0}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n+1-k}.$$

In fact, we will show that the first sum on the LHS here equals the first sum on the RHS, and that the second sum on the LHS equals the second sum on the RHS. In other words, we shall show that

$$\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} = \sum_{k=0}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} \qquad \text{and}$$
$$\sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} = \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n+1-k}.$$

The second of these two equalities is easy, since

$$\sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n+1-k} = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} + \underbrace{\binom{n}{n+1}}_{\substack{=0 \\ (\text{since } n+1>n)}} a^{n+1} b^{n+1-(n+1)}$$
$$= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k}.$$

Remains to prove the first equality:

$$\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} \stackrel{?}{=} \sum_{k=0}^{n+1} \binom{n}{k-1} a^k b^{n+1-k}.$$

The LHS here is

$$\binom{n}{0} a^1 b^n + \binom{n}{1} a^2 b^{n-1} + \cdots + \binom{n}{n} a^{n+1} b^0;$$

the RHS here is

$$\underbrace{\binom{n}{-1}}_{\substack{=0 \\ (\text{since } -1 \notin \mathbb{N})}} a^0 b^{n+1} + \binom{n}{0} a^1 b^n + \binom{n}{1} a^2 b^{n-1} + \cdots + \binom{n}{n} a^{n+1} b^0$$
$$= \binom{n}{0} a^1 b^n + \binom{n}{1} a^2 b^{n-1} + \cdots + \binom{n}{n} a^{n+1} b^0,$$

which is exactly the same sum. So the two sums are equal: they differ only in the presence of the $k = 0$ addends on the RHS, which is 0 and thus does not affect the sum, and in the way they are indexed.

This argument can be made more rigorous using an important summation rule, known as **substitution**. In its simplest form, this rule says that

$$\sum_{k=u}^{v} c_k = \sum_{k=u+\delta}^{v+\delta} c_{k-\delta}$$

for any integers u, v, δ and any numbers $c_u, c_{u+1}, \ldots, c_v$. This is the discrete analogue of the well-known substitution formula

$$\int_u^v f(x)\, dx = \int_{u+\delta}^{v+\delta} f(x-\delta)\, dx$$

from real analysis. When we use the substitution formula to rewrite a sum of the form $\sum_{k=u}^{v} c_k$ as $\sum_{k=u+\delta}^{v+\delta} c_{k-\delta}$, we say that we are **substituting** $k - \delta$ for k.

For example, taking $u = 4$ and $v = 9$ and $c_k = k^k$ and $\delta = -2$, we see that

$$\sum_{k=4}^{9} k^k = \sum_{k=4+(-2)}^{9+(-2)} (k-(-2))^{k-(-2)} = \sum_{k=2}^{7} (k+2)^{k+2}.$$

Now, substituting $k - 1$ for k in the sum $\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k}$, we obtain

$$\begin{aligned}
\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} &= \sum_{k=0+1}^{n+1} \binom{n}{k-1} a^{(k-1)+1} b^{n-(k-1)} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} \\
&= \sum_{k=0}^{n+1} \binom{n}{k-1} a^k b^{n+1-k},
\end{aligned}$$

where in the last step we have extended the sum to start at $k = 0$, which is not a serious change because the new addend for $k = 0$ is just 0.

Either way, we have proved

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.$$

Thus, the induction step is complete, and (BF1) is proved by induction. Thus the whole theorem follows. □

3. Elementary number theory

Number theory commonly means the study of integers, and particular of those properties of integers that are not shared with other kinds of numbers. Divisibility and prime numbers are two such properties. We will cover only the basics of this field here; there are references in the notes if you want to go further.

3.1. Divisibility

3.1.1. Definition

Definition 3.1.1. Let a and b be two integers.

We write $a \mid b$ (and we say that a **divides** b, or b is **divisible by** a, or b is a **multiple of** a, or a is a **divisor** of b) if there exists an integer c such that $b = ac$.

We write $a \nmid b$ for "a does not divide b".

Examples:

- We have $4 \mid 12$, since $12 = 4 \cdot 3$.
- We have $4 \nmid 11$, since there is no integer c such that $11 = 4c$.
- We have $1 \mid b$ for every integer b, since $b = 1b$.
- We have $a \mid a$ for every integer a, since $a = a \cdot 1$. In particular, $0 \mid 0$, even though $0/0$ is not a thing.
- We have $a \mid 0$ for every integer a, since $0 = a \cdot 0$.
- An integer b satisfies $0 \mid b$ if and only if $b = 0$.

Definition 3.1.2. An integer n is said to be **even** if $2 \mid n$, and to be **odd** if $2 \nmid n$.

It is known that

1. a sum of two even numbers is always even;
2. a sum of an even and an odd number is odd;
3. a sum of two odd numbers is even.

The first of these three facts is obvious ($2a + 2b = 2(a + b)$). The second is easy, but the third is not obvious from the definitions. Thus we need to understand divisibility a bit better to prove it. Namely, we need division with remainder. We will cover this soon; first, let us get some basic properties of divisibility out of the way.

3.1.2. Basic properties

Proposition 3.1.3. Let a and b be two integers. Then:

(a) We have $a \mid b$ if and only if $|a| \mid |b|$ (this is saying "$|a|$ divides $|b|$"). In other words, divisibility does not depend on the signs.

(b) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$. In other words, a divisor is never larger than its multiple in absolute value, unless the multiple of 0.

(c) If $a \mid b$ and $b \mid a$, then $|a| = |b|$.

(d) Assume that $a \neq 0$. Then, $a \mid b$ if and only if $\dfrac{b}{a} \in \mathbb{Z}$.

Proof. See the notes.

(a) We need to show that the truth/falsity of $a \mid b$ does not change if we flip the sign of either a or b. In other words, we have to prove that $(a \mid b) \iff (-a \mid b) \iff (a \mid -b)$. Let us merely prove the implication $(a \mid b) \Longrightarrow (a \mid -b)$ (the others are similar). So assume that $a \mid b$. Then, $b = ac$ for some integer c. Hence, $-b = -ac = a(-c)$, and so $a \mid -b$, as desired.

(b) Assume that $a \mid b$ and $b \neq 0$. We must show that $|a| \leq |b|$.

By part **(a)**, from $a \mid b$, we obtain $|a| \mid |b|$. So let $x := |a|$ and $y := |b|$. Then, x and y are nonnegative integers satisfying $x \mid y$ and $y > 0$ (since $b \neq 0$). We must show that $x \leq y$.

We have $x \mid y$, so $y = xz$ for some integer z. Consider this z. If $z \leq 0$, then xz would be ≤ 0 (since $x \geq 0$), which would contradict $xz = y > 0$. So $z > 0$. Since z is an integer, this entails $z \geq 1$. Thus,

$$\begin{aligned} y &= x \underbrace{z}_{\geq 1} \geq x1 \qquad (\text{since } x \geq 0) \\ &= x, \end{aligned}$$

so that $x \leq y$, qed.

(c) First deal with the case when $a = 0$ or $b = 0$ (this case is easy, because any multiple of 0 must itself be 0, so both a and b will be 0 in this case).

In the remaining case, a and b are both nonzero. Hence, part **(b)** yields $|a| \leq |b|$ (since $a \mid b$) and likewise $|b| \leq |a|$ (since $b \mid a$). Combining these inequalities, we get the equality $|a| = |b|$.

(d) We have $b = ac$ if and only if $c = \dfrac{b}{a}$. □

Here are some slightly more substantial rules around divisibility:

Theorem 3.1.4 (rules for divisibility). **(a)** We have $a \mid a$ for each $a \in \mathbb{Z}$. (This is called **reflexivity of divisibility**.)

(b) If $a, b, c \in \mathbb{Z}$ satisfy $a \mid b$ and $b \mid c$, then $a \mid c$. (This is called **transitivity of divisibility**.)

(c) If $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \mid b_1$ and $a_2 \mid b_2$, then $a_1 a_2 \mid b_1 b_2$. (This is called **multiplying two divisibilities**.)

(d) If $d, a, b \in \mathbb{Z}$ satisfy $d \mid a$ and $d \mid b$, then $d \mid a + b$. (This is often restated as "a sum of two multiples of d is again a multiple of d".)

Proof. **(a)** Let $a \in \mathbb{Z}$. Then, there exists a $c \in \mathbb{Z}$ such that $a = ac$. Just take $c = 1$.

(b) Let $a, b, c \in \mathbb{Z}$ be such that $a \mid b$ and $b \mid c$. We must prove that $a \mid c$.

From $a \mid b$, we see that there exists an $x \in \mathbb{Z}$ such that $b = ax$ (by the definition of divisibility).

From $b \mid c$, we see that there exists a $y \in \mathbb{Z}$ such that $c = by$.

Consider these x and y. Now,

$$c = \underbrace{b}_{=ax} y = axy.$$

Since xy is an integer, this entails that $a \mid c$. This proves part **(b)**.

(c) Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \mid b_1$ and $a_2 \mid b_2$. We must prove that $a_1 a_2 \mid b_1 b_2$.

From $a_1 \mid b_1$, we see that $b_1 = a_1 c_1$ for some integer c_1.

From $a_2 \mid b_2$, we see that $b_2 = a_2 c_2$ for some integer c_2.

Using these c_1 and c_2, we have

$$\underbrace{b_1}_{=a_1 c_1} \underbrace{b_2}_{=a_2 c_2} = (a_1 c_1)(a_2 c_2) = (a_1 a_2) \underbrace{(c_1 c_2)}_{\in \mathbb{Z}},$$

so that $a_1 a_2 \mid b_1 b_2$.

(d) Let $d, a, b \in \mathbb{Z}$ satisfy $d \mid a$ and $d \mid b$. We must prove that $d \mid a + b$.

As before, write $a = dx$ and $b = dy$ for integers x and y. Then,

$$a + b = dx + dy = d \underbrace{(x + y)}_{\in \mathbb{Z}},$$

which yields $d \mid a + b$. □

Part **(b)** of the above theorem tells us that divisibilities can be chained together: For example, from $2 \mid 4$ and $4 \mid 12$ and $12 \mid 36$, we obtain $2 \mid 12$ and thus $2 \mid 36$. More generally, if $a_1, a_2, \ldots, a_n$ are n integers, then we shall use the notation $a_1 \mid a_2 \mid \cdots \mid a_n$ to say that "$a_i \mid a_{i+1}$ for each $i \in \{1, 2, \ldots, n-1\}$". Clearly, in this situation, we have $a_1 \mid a_n$ by repeated application of part **(b)** of the theorem.

Another consequence of the above is that a divisibility can be taken to a power: If $a \mid b$, then $a^k \mid b^k$ for each $k \in \mathbb{N}$. To prove this in detail is a homework problem.

3.1.3. Divisibility criteria

How can you spot divisibilites between actual numbers? For small values of a, there are several known **divisibility criteria** (aka **divisibility rules**), which give simple methods to check whether $a \mid b$. Here are a few:

Theorem 3.1.5. Let $b \in \mathbb{N}$. Write b in decimal. Then:
(a) We have $2 \mid b$ if and only if the last digit of b is 0 or 2 or 4 or 6 or 8.
(b) We have $5 \mid b$ if and only if the last digit of b is 0 or 5.
(c) We have $10 \mid b$ if and only if the last digit of b is 0.
(d) We have $3 \mid b$ if and only if the sum of the digits of b is divisible by 3.
(e) We have $9 \mid b$ if and only if the sum of the digits of b is divisible by 9.

Example 3.1.6. Let $b = 10\,835$. Then, $2 \nmid b$, since the last digit is 5. But $5 \mid b$, since the last digit is 5. Likewise, $10 \nmid b$. Do we have $3 \mid b$? The sum of the digits of b is $1 + 0 + 8 + 3 + 5 = 17$, which is not divisible by 3 (itself having sum of digits 8, which is not divisible by 3). Hence, b is not divisible by 3. Thus, b is not divisible by 9 either (because if we had $9 \mid b$, then we would have $3 \mid 9 \mid b$, and thus $3 \mid b$ by transitivity of divisibility).

How do we prove the theorem? Part **(c)** is easy: If you multiply a number (in decimal) by 10, you just insert a digit 0 at its end. For instance, $10 \cdot 39 = 390$. Parts **(a)** and **(b)** are somewhat trickier, and parts **(d)** and **(e)** more so. To give them simple proofs, we will now introduce another kind of relation between integers, known as **congruence modulo** n.

3.2. Congruence modulo n

3.2.1. Definition

Definition 3.2.1. Let $n, a, b \in \mathbb{Z}$. We say that a is **congruent to** b **modulo** n if and only if $n \mid a - b$.

We will use the notation "$a \equiv b \bmod n$" for this.

We will use the notation "$a \not\equiv b \bmod n$" for "a is not congruent to b modulo n".

Example 3.2.2. **(a)** Is $3 \equiv 7 \bmod 12$? No, since this would mean $12 \mid 3 - 7 = -4$, which is not the case.
(b) Is $3 \equiv 7 \bmod 2$? Yes, since $2 \mid 3 - 7 = -4$.
(c) We have $a \equiv b \bmod 1$ for any integers a and b. This is because $1 \mid a - b$.
(d) Two integers a and b satisfy $a \equiv b \bmod 0$ if and only if $a = b$. This is because $0 \mid a - b$ only when $a = b$.
(e) For any two integers a and b, we have $a + b \equiv a - b \bmod 2$. To prove this, note that $(a + b) - (a - b) = 2b$ is divisible by 2.

The word "modulo" in the phrase "a is congruent to b modulo n" originates with Gauss and should be read as something like "with respect to". The definition of congruence can be restated as follows:

$$a \equiv b \bmod n \qquad \text{if and only if} \qquad a = b + nc \text{ for some } c \in \mathbb{Z}.$$

As we will soon, congruence modulo 2 is essentially parity:

- Two even numbers are always congruent modulo 2.
- Two odd numbers are always congruent modulo 2.
- An even number is never congruent to an odd number modulo 2.

We will prove this soon.

3.2.2. Basic properties

Proposition 3.2.3. Let $n, a \in \mathbb{Z}$. Then, $a \equiv 0 \bmod n$ if and only if $n \mid a$.

Proof. We have $a \equiv 0 \bmod n$ if and only if $n \mid a - 0$, but this simplifies to $n \mid a$. □

Proposition 3.2.4 (rules for congruence)**.** Let $n \in \mathbb{Z}$. Then:
(a) We have $a \equiv a \bmod n$ for every $a \in \mathbb{Z}$. (This is called the **reflexivity of congruence**.)
(b) If $a, b \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$, then $b \equiv a \bmod n$. (This is called **symmetry of congruence**.)
(c) If $a, b, c \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$. (This is called **transitivity of congruence**.)
(d) If $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy

$$a_1 \equiv b_1 \bmod n \qquad \text{and} \qquad a_2 \equiv b_2 \bmod n,$$

then

$$\begin{aligned} a_1 + a_2 &\equiv b_1 + b_2 \bmod n; \\ a_1 - a_2 &\equiv b_1 - b_2 \bmod n; \\ a_1 a_2 &\equiv b_1 b_2 \bmod n. \end{aligned}$$

(In other words, two congruences modulo n can be added, subtracted or multiplied.)

(e) Let $m \in \mathbb{Z}$ be such that $m \mid n$. If $a, b \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$, then $a \equiv b \bmod m$.

Proof. **(a)** Let $a \in \mathbb{Z}$. Then, $a \equiv a \bmod n$, since $n \mid a - a$, because $a - a = 0$ is divisible by everything.

(b) Let $a, b \in \mathbb{Z}$ be such that $a \equiv b \bmod n$. We must prove that $b \equiv a \bmod n$.

Our assumption $a \equiv b \bmod n$ can be rewritten as $n \mid a - b$. This entails $n \mid b - a$ since $b - a = -(a - b)$ and the sign is irrelevant in a divisibility. But this means that $b \equiv a \bmod n$.

(c) Let $a, b, c \in \mathbb{Z}$ be such that $a \equiv b \bmod n$ and $b \equiv c \bmod n$. We must show that $a \equiv c \bmod n$.

From $a \equiv b \bmod n$, we obtain $n \mid a - b$. That is, $a - b$ is a multiple of n. Similarly, $b - c$ is a multiple of n. Hence, their sum $(a - b) + (b - c)$ is also a multiple of n (by the divisibility rule "a sum of two multiples of d is again a multiple of d"). But this sum is just $a - c$. So we proved $n \mid a - c$, which means $a \equiv c \bmod n$.

(d) Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy

$$a_1 \equiv b_1 \bmod n \qquad \text{and} \qquad a_2 \equiv b_2 \bmod n.$$

We must prove that

$$\begin{aligned} a_1 + a_2 &\equiv b_1 + b_2 \bmod n; \\ a_1 - a_2 &\equiv b_1 - b_2 \bmod n; \\ a_1 a_2 &\equiv b_1 b_2 \bmod n. \end{aligned}$$

From $a_1 \equiv b_1 \bmod n$, we obtain $n \mid a_1 - b_1$, so that $a_1 - b_1 = nc_1$ for some integer c_1. Consider this c_1, and conclude that $a_1 = b_1 + nc_1$. Likewise, $a_2 = b_2 + nc_2$ for some integer c_2. We can use these two equalities to rewrite a_1, a_2 in terms of b_1, b_2, c_1, c_2 and forget about the congruences. We have

$$\begin{aligned} a_1 + a_2 &= (b_1 + nc_1) + (b_2 + nc_2) \\ &= (b_1 + b_2) + n(c_1 + c_2), \end{aligned}$$

so that $a_1 + a_2$ differs from $b_1 + b_2$ by a multiple of n (namely, $n(c_1 + c_2)$). Thus,

$$a_1 + a_2 \equiv b_1 + b_2 \bmod n.$$

Likewise,

$$\begin{aligned} a_1 - a_2 &= (b_1 + nc_1) - (b_2 + nc_2) \\ &= (b_1 - b_2) + n(c_1 - c_2), \end{aligned}$$

and thus $a_1 - a_2 \equiv b_1 - b_2 \bmod n$.

Finally,

$$\begin{aligned} a_1 a_2 &= (b_1 + nc_1)(b_2 + nc_2) \\ &= b_1 b_2 + b_1 nc_2 + nc_1 b_2 + nc_1 nc_2 \\ &= b_1 b_2 + n(b_1 c_2 + c_1 b_2 + c_1 nc_2), \end{aligned}$$

and thus $a_1 a_2 \equiv b_1 b_2 \bmod n$. So everything is shown.

(e) Assume that $a, b \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$. We must show that $a \equiv b \bmod m$.

From $a \equiv b \bmod n$, we obtain $n \mid a - b$. Now, $m \mid n \mid a - b$. Thus, by transitivity of divisibility, $m \mid a - b$, so that $a \equiv b \bmod m$. □

All five parts of the above theorem are very useful:

- Part **(b)** says that congruences can be turned around: From $a \equiv b \bmod n$, we can always obtain $b \equiv a \bmod n$. (This is in contrast to divisibilities, where $a \mid b$ is very different from $b \mid a$.)
- Part **(c)** says that congruences can be chained together: From $a \equiv b \bmod n$ and $b \equiv c \bmod n$, we obtain $a \equiv c \bmod n$. This prompts a certain notation: The "chain of congruences"

  $$a_1 \equiv a_2 \equiv \cdots \equiv a_k \bmod n$$

  means that each of the numbers $a_1, a_2, \ldots, a_k$ is congruent to the next modulo n (that is, $a_i \equiv a_{i+1} \bmod n$ for each $i \in \{1, 2, \ldots, k-1\}$). By transitivty, this entails that $a_1 \equiv a_k \bmod n$ and $a_i \equiv a_j \bmod n$ for all i, j.

  Note: Two congruences can only be chained together if they are modulo the same n. For instance, $1 \equiv 4 \bmod 3$ and $4 \equiv 2 \bmod 2$ but $1 \not\equiv 2 \bmod$ either.
- Part **(d)** allows addition, subtraction and multiplication of congruences. But exponentiation and division don't work. For instance, $2 \equiv 2 \bmod 2$ and $2 \equiv 0 \bmod 2$ but $2^2 \not\equiv 2^0 \bmod 2$.

  At least you can take a congruence to the k-th power: If $a \equiv b \bmod n$, then $a^k \equiv b^k \bmod n$ for each $k \in \mathbb{N}$. This is obtained by multiplying the congruence $a \equiv b \bmod n$ with itself k times. (Detailed proof to be done in homework.)
- Part **(e)** says that the n in a congruence $a \equiv b \bmod n$ can be replaced by any divisor of n.

3.2.3. Proving the divisibility criteria

Now let us prove the divisibility criterion for 9, restating it as follows:

Proposition 3.2.5. Let $m \in \mathbb{N}$. Let s be the sum of the digits of m written in decimal. (For instance, if $m = 302$, then $s = 3 + 0 + 2 = 5$.)
Then, $9 \mid m$ if and only if $9 \mid s$.

Proof. Let the integer m have decimal representation $m_d m_{d-1} \cdots m_1 m_0$ (where m_d is the leading digit). Thus,

$$\begin{aligned} m &= m_d \cdot 10^d + m_{d-1} \cdot 10^{d-1} + \cdots + m_0 \cdot 10^0; \\ s &= m_d + m_{d-1} + \cdots + m_0. \end{aligned}$$

However, $10 \equiv 1 \bmod 9$ (since $9 \mid 10 - 1 = 9$). Hence, taking this congruence to the k-th power, we obtain

$$10^k \equiv 1^k \bmod 9 \qquad \text{for each } k \in \mathbb{N}.$$

Multiplying this further with the obvious congruence $m_k \equiv m_k \bmod 9$, we obtain

$$m_k \cdot 10^k \equiv m_k \cdot 1^k \bmod 9,$$

which simplifies to

$$m_k \cdot 10^k \equiv m_k \bmod 9.$$

In other words,

$$\begin{aligned} m_d \cdot 10^d &\equiv m_d \bmod 9; \\ m_{d-1} \cdot 10^{d-1} &\equiv m_{d-1} \bmod 9; \\ &\ldots; \\ m_0 \cdot 10^0 &\equiv m_0 \bmod 9. \end{aligned}$$

Adding these $d + 1$ congruences together, we obtain

$$m_d \cdot 10^d + m_{d-1} \cdot 10^{d-1} + \cdots + m_0 \cdot 10^0 \equiv m_d + m_{d-1} + \cdots + m_0 \bmod 9.$$

In other words,

$$m \equiv s \bmod 9.$$

Now, our goal is to show that $9 \mid m$ if and only if $9 \mid s$. In other words, we must show that $m \equiv 0 \bmod 9$ if and only if $s \equiv 0 \bmod 9$. But this is now easy:

- If $m \equiv 0 \bmod 9$, then $m \equiv s \bmod 9$ entails $s \equiv m \equiv 0 \bmod 9$ and therefore $s \equiv 0 \bmod 9$ by transitivity of congruence.
- If $s \equiv 0 \bmod 9$, then $m \equiv s \equiv 0 \bmod 9$ and thus $m \equiv 0 \bmod 9$ by transitivity of congruence.

We have now proved the divisibility rule for 9. □

This also yields the divisibility rule for 3, since $m \equiv s \bmod 9$ entails $m \equiv s \bmod 3$.

The other divisibility rules (for 2, 5 and 10) are simpler.

There is also a divisibility rule for 11 (homework problem!).

3.3. Division with remainder

3.3.1. The theorem

What comes next is the most fundamental theorem of number theory:

Theorem 3.3.1 (division-with-remainder theorem)**.** Let n be an integer. Let d be a positive integer. Then, there exists a **unique** pair (q, r) of integers

$$q \in \mathbb{Z} \qquad \text{and} \qquad r \in \{0, 1, \ldots, d-1\}$$

such that

$$n = qd + r.$$

We will prove this soon, but let us first give these two numbers q and r names:

Definition 3.3.2. Let n be an integer. Let d be a positive integer. Consider the unique pair (q, r) constructed in the previous theorem. Then:

- The number q is called the **quotient** of the division of n by d, and will be denoted by $n//d$. (Some call it `quo(n,d)`.)
- The number r is called the **remainder** of the division of n by d, and will be denoted by $n\%d$. (Some call it `rem(n,d)` or `n mod d`.)
- The pair (q, r) is called the **quo-rem pair** of n and d.

For now, we don't actually know that this quo-rem pair (q, r) exists and is unique. So we will talk about "**a** quo-rem pair of n and d" until we have proved its existence and uniqueness.

Example 3.3.3. What are $8//5$ and $8\%5$? We have

$$8 = 1 \cdot 5 + 3,$$

so $8//5 = 1$ and $8\%5 = 3$.

Example 3.3.4. What are $19//5$ and $19\%5$? We have

$$19 = 3 \cdot 5 + 4,$$

so $19//5 = 3$ and $19\%5 = 4$.

Example 3.3.5. What are $(-7)//5$ and $(-7)\%5$? We have

$$-7 = (-2) \cdot 5 + 3,$$

so $(-7)//5 = -2$ and $(-7)\%5 = 3$.

3.3.2. The proof

Proof of the theorem. We must prove that there exists a unique quo-rem pair of n and d. Let me start by proving the uniqueness:

Proof of the uniqueness. We must show that there is **at most one** quo-rem pair of n and d. In other words, we must show that any two quo-rem pairs of n and d are necessarily equal.

So let (q_1, r_1) and (q_2, r_2) be two quo-rem pairs of n and d. We must show that $(q_1, r_1) = (q_2, r_2)$. That is, we must show that $q_1 = q_2$ and $r_1 = r_2$.

Since (q_1, r_1) is a quo-rem pair of n and d, we have

$$q_1 \in \mathbb{Z} \qquad \text{and} \qquad r_1 \in \{0, 1, \ldots, d-1\} \qquad \text{and} \qquad n = q_1 d + r_1.$$

Likewise,

$$q_2 \in \mathbb{Z} \qquad \text{and} \qquad r_2 \in \{0, 1, \ldots, d-1\} \qquad \text{and} \qquad n = q_2 d + r_2.$$

We have

$$q_1 d + r_1 = n = q_2 d + r_2,$$

so that

$$q_1 d - q_2 d = r_2 - r_1,$$

so that

$$(q_1 - q_2)\, d = r_2 - r_1.$$

But this equality can only hold if both sides are 0. In fact:

- The LHS is a multiple of d, so it is one of the numbers $\ldots, -2d, -d, 0, d, 2d, \ldots$.
- The RHS is a difference of two elements $r_2, r_1 \in \{0, 1, \ldots, d-1\}$, so it is one of the numbers $-d+1, -d+2, \ldots, d-2, d-1$.

Thus, the LHS and the RHS can only be equal if they are both 0, since the sets of numbers have nothing but 0 in common. That is, both $(q_1 - q_2)\,d$ and $r_2 - r_1$ are 0. Since $d \neq 0$, this entails that $q_1 - q_2 = 0$ as well. So $q_1 = q_2$ and $r_1 = r_2$ since $r_2 - r_1 = 0$. Therefore, $(q_1, r_1) = (q_2, r_2)$, as desired. This shows that the quo-rem pair of n, d is unique if it exists.

(See the notes for a more computational way of wording this proof.) □

It remains to prove the existence of such a quo-rem pair. We shall do this by strong induction on n. However, there is a little twist, in that our statement allows n to be an arbitrary integer, whereas induction only goes upwards from the base case. So we need to handle the case of nonnegative n first (this can be done by strong induction), and then extend the result to the negative case.

We state the nonnegative case as a lemma, which is actually a bit stronger because it says that $q \in \mathbb{N}$ rather than just $q \in \mathbb{Z}$. □

Lemma 3.3.6. Let $n \in \mathbb{N}$, and let d be a positive integer. Then, there exists a quo-rem pair (q, r) of n and d with $q \in \mathbb{N}$.

Proof. Fix d (but not n). Apply strong induction on n. We use the baseless form of strong induction, so we need no base case (even though the case $n = 0$ would be easy: here, $(q, r) = (0, 0)$).

Induction step: Let $n \in \mathbb{N}$. Assume (as the IH) that the lemma is proved for all nonnegative integers smaller than n. In other words, for each nonnegative integer $k < n$, there exists a quo-rem pair of k and d and its first entry is nonnegative. Now we must prove the same for n. So we must show that there exists a quo-rem pair (q, r) of n and d with $q \in \mathbb{N}$.

If $n < d$, then the desired quo-rem pair is $(0, n)$, since $n \in \{0, 1, \ldots, d-1\}$ and $0 \in \mathbb{N}$ and $n = 0d + n$.

Otherwise, $n \geq d$. In this case, $n - d$ is a nonnegative integer smaller than n (since $d > 0$). Hence, we can apply the IH to $n - d$. We conclude that there exists a quo-rem pair (q', r') of $n - d$ and d with $q' \in \mathbb{N}$. Consider this pair. So $q' \in \mathbb{N}$ and $r' \in \{0, 1, \ldots, d-1\}$ and $n - d = q'd + r'$. Hence,

$$n = q'd + r' + d = \left(q' + 1\right) d + r'.$$

Now $(q' + 1, r')$ is a quo-rem pair of n and d. Thus, n and d have a quo-rem pair, and we are done with the induction step.

Therefore the lemma is proved by induction. □

Proof of the theorem, continued. Uniqueness was already proved above.

The above lemma proves existence in the case $n \in \mathbb{N}$.

It remains to prove existence when $n < 0$. This can be done by strong induction on $-n$, similarly to how we proved the lemma above. (This time we use $n + d$ instead of $n - d$.)

Alternatively, there is a trick which allows us to reduce the negative case to the positive (nonnegative) case: Namely, let $n \in \mathbb{Z}$ be negative. Then,

$\underbrace{(1-d)}_{\leq 0}\underbrace{n}_{<0}$ is nonnegative. Thus, we can apply the lemma to $(1-d)\,n$ instead of n. We conclude that there is a quo-rem pair (q', r') for $(1-d)\,n$ and d. Thus,

$$(1-d)\,n = q'd + r'.$$

Equivalently,

$$\begin{aligned} n - dn &= q'd + r', \qquad \text{so that} \\ n &= q'd + r' + dn = \left(q' + n\right) d + r'. \end{aligned}$$

Therefore, $(q' + n, r')$ is a quo-rem pair for n and d. So a quo-rem pair exists even in the negative case, and thus the proof of the theorem is complete. □

3.3.3. Application: even and odd integers

Recall that an integer n is called **even** or **odd** if $2 \mid n$ or $2 \nmid n$, respectively. Now we shall show:

Proposition 3.3.7. Let n be an integer.
(a) The integer n is even if and only if $n = 2k$ for some $k \in \mathbb{Z}$.
(b) The integer n is odd if and only if $n = 2k+1$ for some $k \in \mathbb{Z}$.

Proof. **(a)** Trivial consequence of our definition of divisibility.
(b) This is an "if and only if" statement, so it makes the two claims

$$(n \text{ is odd}) \Longrightarrow (n = 2k+1 \text{ for some } k \in \mathbb{Z})$$

and

$$(n \text{ is odd}) \Longleftarrow (n = 2k+1 \text{ for some } k \in \mathbb{Z}).$$

Let us prove these two claims separately.

$\Longrightarrow$: Assume that n is odd. We must show that $n = 2k+1$ for some $k \in \mathbb{Z}$.

By the theorem above, there is a quo-rem pair (q, r) of n and 2. Consider it. Then, $r \in \{0, 1\}$ and $q \in \mathbb{Z}$ and $n = q \cdot 2 + r$. But $r = 0$ is impossible, since this would yield $n = q \cdot 2 + 0 = 2q$ in contradiction to n being odd. So we must have $r = 1$, since $r \in \{0, 1\}$. Thus, $n = q \cdot 2 + r$ becomes $n = 2q + 1$, so that $n = 2k+1$ for some $k \in \mathbb{Z}$ (namely, $k = q$). This proves the "$\Longrightarrow$" direction.

$\Longleftarrow$: Assume that $n = 2k+1$ for some $k \in \mathbb{Z}$. We must show that n is odd.

Assume the contrary. Thus, n is even, i.e., we have $2 \mid n$. This means that $n = 2q$ for some $q \in \mathbb{Z}$. So $n = 2q = 2q + 0$, which shows that $(q, 0)$ is a quo-rem pair for n and 2. But $n = 2k+1$ shows that $(k, 1)$ is a quo-rem pair for n and 2. Thus, n and 2 have two different quo-rem pairs: $(q, 0)$ and $(k, 1)$. But this is impossible, since quo-rem pairs are unique (by the above theorem). So we got our contradiction, and have proved the "$\Longleftarrow$" direction.

Thus, part **(b)** is proved. □

Corollary 3.3.8. **(a)** The sum of any two even integers is even.
(b) The sum of an even and an odd integer is odd.
(c) The sum of any two odd integers is even.

Proof. **(c)** Let a and b be two odd integers. We must show that $a+b$ is even.

By part **(b)** of the previous proposition, we can write a and b as $a = 2k+1$ and $b = 2\ell+1$ for some $k, \ell \in \mathbb{Z}$. Then, we get

$$a+b = (2k+1)+(2\ell+1) = 2(k+\ell+1),$$

which is visibly even. So we are done with part **(c)**.

(a), **(b)** are similar. □

Note that part **(c)** is specific to the number 2. In contrast, if a and b are two integers that are not divisible by 3, then $a+b$ may or may not be divisible by 3.

3.3.4. Basic properties of quotients and remainders

Proposition 3.3.9. Let $n \in \mathbb{Z}$, and let d be a positive integer. Then:
(a) We have $n\%d \in \{0,1,\ldots,d-1\}$ and $n\%d \equiv n \bmod d$.
(b) We have $d \mid n$ if and only if $n\%d = 0$.
(c) If $c \in \{0,1,\ldots,d-1\}$ satisfies $c \equiv n \bmod d$, then $c = n\%d$.
(d) We have $n = (n//d)\,d + (n\%d)$.
(e) If $n \in \mathbb{N}$, then $n//d \in \mathbb{N}$.

Proof. Let $q = n//d$ and $r = n\%d$. Thus, (q,r) is a quo-rem pair of n and d. In other words,

$$q \in \mathbb{Z} \qquad \text{and} \qquad r \in \{0,1,\ldots,d-1\} \qquad \text{and} \qquad n = qd+r.$$

(a) We must prove that $r \in \{0,1,\ldots,d-1\}$ and $r \equiv n \bmod d$. The former is obvious. The latter follows from $r - \underbrace{n}_{=qd+r} = r-(qd+r) = d(-q)$, which is clearly a multiple of d.

(b) We must prove that $d \mid n$ if and only if $r = 0$.

The "if" part is easy: If $r = 0$, then $n = qd + \underbrace{r}_{=0} = qd$, which is clearly divisible by d; thus $d \mid n$ holds.

For the "only if" part: We assume that $d \mid n$ and try to prove that $r = 0$.

But $d \mid n$, so that $n = dk$ for some $k \in \mathbb{Z}$. Therefore, $(k,0)$ is a quo-rem pair of n and d (since $n = dk = kd+0$). Since (q,r) is a quo-rem pair of n and d as well, this entails that $(k,0) = (q,r)$, since quo-rem pairs are unique. In particular, $0 = r$, so that $r = 0$.

(c) Let $c \in \{0,1,\ldots,d-1\}$ satisfy $c \equiv n \bmod d$. We must prove that $c = n\%d$, that is, $c = r$.

We have $c \equiv n \bmod d$, so that $d \mid c - n$. In other words, $c - n = dp$ for some $p \in \mathbb{Z}$. Solving this equality by n, we obtain $n = c - dp = (-p)\, d + c$. Thus, $(-p, c)$ is a quo-rem pair of n and d (since $c \in \{0, 1, \ldots, d-1\}$). But (q, r) is a quo-rem pair of n and d as well. By the uniqueness of quo-rem pairs, we thus conclude $(-p, c) = (q, r)$. In particular, $c = r$, qed.

(d) This is just saying that $n = qd + r$, but this is clear.

(e) This follows from the lemma above. □

Corollary 3.3.10. Let $n \in \mathbb{Z}$. Then:

(a) The integer n is even if and only if $n\%2 = 0$.

(b) The integer n is odd if and only if $n\%2 = 1$.

Proof. Follows easily from part **(b)** of the above proposition, since the remainder $n\%2$ can only be 0 or 1. □

Quotients and remainders are closely connected to the so-called floor function (or rounding-down function):

Definition 3.3.11. The **integer part** (or **floor**) of a real number x is defined to be the largest integer that is $\leq x$. It is denoted by $\lfloor x \rfloor$.

For instance,

$$\lfloor 3.8 \rfloor = 3, \qquad \lfloor 4.2 \rfloor = 4, \qquad \lfloor 5 \rfloor = 5, \qquad \left\lfloor \sqrt{2} \right\rfloor = 1,$$
$$\lfloor \pi \rfloor = 3, \qquad \lfloor 0.5 \rfloor = 0, \qquad \lfloor -1.2 \rfloor = -2.$$

Now we can connect floors to quotients and remainders:

Proposition 3.3.12. Let $n \in \mathbb{Z}$, and let d be a positive integer. Then,

$$n//d = \left\lfloor \frac{n}{d} \right\rfloor \qquad \text{and} \qquad n\%d = n - d \left\lfloor \frac{n}{d} \right\rfloor.$$

Proof. The second equation follows from the first by solving the equation $n = (n//d)\, d + (n\%d)$ for $n\%d$. Thus it remains to prove the first equation.

We must prove that $n//d = \left\lfloor \frac{n}{d} \right\rfloor$. It suffices to show that

$$n//d \leq \frac{n}{d} < (n//d) + 1.$$

Multiplying this inequality by d, we rewrite it as

$$(n//d)\, d \leq n < (n//d)\, d + d.$$

But this follows from $n = (n//d)\, d + \underbrace{(n\%d)}_{\in \{0,1,\ldots,d-1\}}$.

(Details in the notes: Proposition 3.3.14.) □

3.3.5. Base-b representation of nonnegative integers

Division with remainder is the main ingredient in a feature of integers that you are well familiar with: the fact that each integer can be uniquely expressed in decimal notation, or, more generally, in base-b notation for any given integer $b > 1$.

What does this mean? For example,

$$\begin{aligned} 3401 &= 3 \cdot 1000 + 4 \cdot 100 + 0 \cdot 10 + 1 \cdot 1 \\ &= 3 \cdot 10^3 + 4 \cdot 10^2 + 0 \cdot 10^1 + 1 \cdot 10^0. \end{aligned}$$

This can be done for any nonnegative integer instead of 3401 and any integer $b > 1$ instead of 10. This is called "base-b representation".

For instance, let us find the base-4 representation of the integer 3401. This will be a way of writing 3401 as a sum

$$3401 = r_6 \cdot 4^6 + r_5 \cdot 4^5 + r_4 \cdot 4^4 + r_3 \cdot 4^3 + r_2 \cdot 4^2 + r_1 \cdot 4^1 + r_0 \cdot 4^0,$$

where each r_i is a "base-4 digit", i.e., an element of $\{0, 1, 2, 3\}$. We might actually need more than 7 digits, but let's hope that 7 is enough.

How do we find these 7 digits $r_6, r_5, \ldots, r_0$? We have

$$\begin{aligned} 3401 &= r_6 \cdot 4^6 + r_5 \cdot 4^5 + r_4 \cdot 4^4 + r_3 \cdot 4^3 + r_2 \cdot 4^2 + r_1 \cdot 4^1 + r_0 \cdot 4^0 \\ &= 4 \cdot \left(r_6 \cdot 4^5 + r_5 \cdot 4^4 + r_4 \cdot 4^3 + r_3 \cdot 4^2 + r_2 \cdot 4^1 + r_1 \cdot 4^0 \right) + r_0 \cdot \underbrace{4^0}_{=1} \\ &= 4 \cdot \left(r_6 \cdot 4^5 + r_5 \cdot 4^4 + r_4 \cdot 4^3 + r_3 \cdot 4^2 + r_2 \cdot 4^1 + r_1 \cdot 4^0 \right) + r_0. \end{aligned}$$

This equality (along with the fact that $r_0 \in \{0, 1, 2, 3\}$) shows that

$$\left(r_6 \cdot 4^5 + r_5 \cdot 4^4 + r_4 \cdot 4^3 + r_3 \cdot 4^2 + r_2 \cdot 4^1 + r_1 \cdot 4^0,\ r_0 \right)$$

is a quo-rem pair for 3401 and 4. In particular,

$$\begin{aligned} r_0 &= 3401 \% 4 = 1; \\ r_6 \cdot 4^5 + r_5 \cdot 4^4 + r_4 \cdot 4^3 + r_3 \cdot 4^2 + r_2 \cdot 4^1 + r_1 \cdot 4^0 &= 3401 // 4 = 850. \end{aligned}$$

So we found r_0. What next? We have

$$\begin{aligned} 850 &= r_6 \cdot 4^5 + r_5 \cdot 4^4 + r_4 \cdot 4^3 + r_3 \cdot 4^2 + r_2 \cdot 4^1 + r_1 \cdot 4^0 \\ &= 4 \cdot \left(r_6 \cdot 4^4 + r_5 \cdot 4^3 + r_4 \cdot 4^2 + r_3 \cdot 4^1 + r_2 \cdot 4^0 \right) + r_1, \end{aligned}$$

so that

$$\begin{aligned} r_1 &= 850 \% 4 = 2; \\ r_6 \cdot 4^4 + r_5 \cdot 4^3 + r_4 \cdot 4^2 + r_3 \cdot 4^1 + r_2 \cdot 4^0 &= 850 // 4 = 212. \end{aligned}$$

So we found r_1. Next,

$$\begin{aligned} 212 &= r_6 \cdot 4^4 + r_5 \cdot 4^3 + r_4 \cdot 4^2 + r_3 \cdot 4^1 + r_2 \cdot 4^0 \\ &= 4 \cdot \left(r_6 \cdot 4^3 + r_5 \cdot 4^2 + r_4 \cdot 4^1 + r_3 \cdot 4^0 \right) + r_2, \end{aligned}$$

so that

$$\begin{aligned} r_2 &= 212\%4 = 0; \\ r_6 \cdot 4^3 + r_5 \cdot 4^2 + r_4 \cdot 4^1 + r_3 \cdot 4^0 &= 212//4 = 53. \end{aligned}$$

Another digit found. Similarly, we go on to find

$$r_3 = 1 \qquad \text{and} \qquad r_6 \cdot 4^2 + r_5 \cdot 4^1 + r_4 \cdot 4^0 = 13.$$

Next,

$$r_4 = 1 \qquad \text{and} \qquad r_6 \cdot 4^1 + r_5 \cdot 4^0 = 3;$$

then

$$r_5 = 3 \qquad \text{and} \qquad r_6 \cdot 4^0 = 0.$$

Finally,

$$r_6 = 0.$$

So

$$\begin{aligned} 3401 &= \underbrace{0 \cdot 4^6}_{=0} + 3 \cdot 4^5 + 1 \cdot 4^4 + 1 \cdot 4^3 + 0 \cdot 4^2 + 2 \cdot 4^1 + 1 \cdot 4^0 \\ &= 3 \cdot 4^5 + 1 \cdot 4^4 + 1 \cdot 4^3 + 0 \cdot 4^2 + 2 \cdot 4^1 + 1 \cdot 4^0. \end{aligned}$$

In other words, the base-4 representation of 3401 is $\overline{311021}_4$.

Let us generalize this method. We obtain an algorithm that can be used for any integer $b > 1$ instead of 4 and any nonnegative integer n instead of 3401: To find the base-b digits of n, we first divide n by b with remainder, then divide the resulting quotient again by b with remainder, then divide the resulting quotient again by b with remainder, and so on, until we are left with the quotient 0. The remainders obtained in this process will be the base-b digits of n (from right to left). This process must eventually come to an end, since each quotient will be smaller than the preceding one (here we use $b > 1$, which ensures $m//b < m$ for all $m > 0$).

We summarize this as a theorem, saying a bit more:

Theorem 3.3.13. Let $b > 1$ be an integer. Let $n \in \mathbb{N}$. Then:
(a) We can write n in the form

$$n = r_k \cdot b^k + r_{k-1} \cdot b^{k-1} + \cdots + r_1 \cdot b^1 + r_0 \cdot b^0$$

with

$$k \in \mathbb{N} \qquad \text{and} \qquad r_0, r_1, \ldots, r_k \in \{0, 1, \ldots, b-1\}.$$

(b) If $n < b^{k+1}$ for some $k \in \mathbb{N}$, then we can write n in the form

$$n = r_k \cdot b^k + r_{k-1} \cdot b^{k-1} + \cdots + r_1 \cdot b^1 + r_0 \cdot b^0$$

with

$$r_0, r_1, \ldots, r_k \in \{0, 1, \ldots, b-1\}.$$

(c) These $r_0, r_1, \ldots, r_k$ are unique (when k is given). Moreover, there is an explicit formula for them:

$$r_i = \left(n // b^i\right) \% b \qquad \text{for each } i \in \{0, 1, \ldots, k\}.$$

That is,

$$\begin{aligned} r_0 &= n \% b, \\ r_1 &= (n // b) \% b, \\ r_2 &= \left(n // b^2\right) \% b, \\ &\cdots. \end{aligned}$$

Proof. See the notes. Note that the formula in **(c)** is not quite what our above method yields, but it is equivalent (in fact, it can be shown that $n // b^i = ((((n // b) // b) // b) // \cdots) // b$ with i many divisions). □

3.3.6. Congruence in terms of remainders

Here is an application of division with remainder: a new criterion for congruence:

Proposition 3.3.14. Let d be a positive integer. Let a and b be two integers. Then,

$$a \equiv b \bmod d \qquad \text{if and only if} \qquad a\%d = b\%d.$$

Proof. We know that $a\%d \in \{0, 1, \ldots, d-1\}$ and $a\%d \equiv a \bmod d$. Similarly, $b\%d \in \{0, 1, \ldots, d-1\}$ and $b\%d \equiv b \bmod d$.

Now, if $a \equiv b \bmod d$, then we obtain

$$a\%d \equiv a \equiv b \equiv b\%d \bmod d$$

(since congruence mod d is symmetric, so $b\%d \equiv b \bmod d$ entails $b \equiv b\%d \bmod d$), whence $a\%d = b\%d$ (since both $a\%d$ and $b\%d$ belong to the length-d interval

$\{0, 1, \ldots, d-1\}$, which is too short to contain two numbers that are a nonzero multiple of d apart).

Thus we have shown that $a \equiv b \bmod d$ entails $a\%d = b\%d$. The converse follows similarly:

$$a \equiv a\%d = b\%d \equiv b \bmod d.$$

□

Corollary 3.3.15. Let a and b be two integers. Then, $a \equiv b \bmod 2$ if and only if the numbers a and b are either both even or both odd.

Proof. Apply the proposition to $d = 2$. This shows that $a \equiv b \bmod 2$ if and only if $a\%2 = b\%2$. But $a\%2 = \begin{cases} 0, & \text{if } a \text{ is even;} \\ 1, & \text{if } a \text{ is odd} \end{cases}$ and $b\%2 = \begin{cases} 0, & \text{if } b \text{ is even;} \\ 1, & \text{if } b \text{ is odd.} \end{cases}$ Thus, the equation $a\%2 = b\%2$ is simply saying that a and b are even/odd together. □

3.3.7. The birthday lemma

If you have lived for exactly n days, then you are $n//365$ years and $n\%365$ days old (assuming for simplicity that there are no leap years). On any "normal" day, the latter number ($n\%365$) increases by 1 while the former number ($n//365$) remains unchanged. On a birthday, however, the number $n\%365$ gets reset to 0, while $n//365$ increases by 1. This holds more generally for any d instead of 365:

Proposition 3.3.16 (birthday lemma)**.** Let $n \in \mathbb{Z}$, and let d be a positive integer. Then:

(a) If $d \mid n$, then

$$n//d = ((n-1)//d) + 1 \qquad \text{and}$$
$$n\%d = 0 \qquad \text{and} \qquad (n-1)\%d = d-1.$$

(b) If $d \nmid n$, then

$$n//d = (n-1)//d \qquad \text{and}$$
$$n\%d = ((n-1)\%d) + 1.$$

Proof. See the notes. Nothing surprising here. □

We can, of course, rewrite the quotient part of the proposition using floors:

$$\left\lfloor \frac{n}{d} \right\rfloor = \left\lfloor \frac{n-1}{d} \right\rfloor + 1 \qquad \text{if } d \mid n;$$
$$\left\lfloor \frac{n}{d} \right\rfloor = \left\lfloor \frac{n-1}{d} \right\rfloor \qquad \text{if } d \nmid n.$$

3.4. Greatest common divisors

3.4.1. Definition

The following definition plays a crucial role in number theory.

Definition 3.4.1. Let a and b be two integers.

(a) The **common divisors** of a and b are the integers that divide a and simultaneously divide b.

(b) The **greatest common divisor** of a and b is the largest among the common divisors of a and b, unless $a = b = 0$. In this case, it is 0 by definition (since there is no greatest integer).

We denote the greatest common divisor of a and b by $\gcd(a,b)$, and we even call it the **gcd** of a and b.

Some examples:

- What is $\gcd(4,6)$?

  The divisors of 4 are $-4,-2,-1,1,2,4$.

  The divisors of 6 are $-6,-3,-2,-1,1,2,3,6$.

  The common divisors of 4 and 6 are $-2,-1,1,2$.

  The greatest common divisor of 4 and 6 is therefore 2. That is, $\gcd(4,6) = 2$.

- What is $\gcd(0,5)$?

  The divisors of 0 are all the integers.

  The divisors of 5 are $-5,-1,1,5$.

  The common divisors of 0 and 5 are $-5,-1,1,5$.

  Thus, $\gcd(0,5) = 5$.

- As we said, $\gcd(0,0) = 0$ by definition, even though there is no literally greatest among the common divisors of 0 and 0.

Remark 3.4.2. Why is $\gcd(a,b)$ well-defined?

For $a = b = 0$, this is because we just defined it to be 0.

In all other cases, at least one of a and b is nonzero and thus has finitely many divisors (in fact, any divisor of a nonzero integer c lies in $\{-c, -c+1, \ldots, c-1, c\}$, which is finite). So there are only finitely many common divisors of a and b. The other thing that could go wrong would be that there are no common divisors of a and b. But this doesn't happen, since 1 is always a common divisor of a and b.

This argument gives us a slow and stupid algorithm for computing $\gcd(a,b)$. We will see a better one soon.

3.4.2. Basic properties

Proposition 3.4.3. **(a)** We have $\gcd(a,b) \in \mathbb{N}$ for any $a, b \in \mathbb{Z}$.
(b) We have $\gcd(a,0) = \gcd(0,a) = |a|$ for any $a \in \mathbb{Z}$.
(c) We have $\gcd(a,b) = \gcd(b,a)$ for any $a, b \in \mathbb{Z}$.
(d) If $a, b, c \in \mathbb{Z}$ satisfy $b \equiv c \bmod a$, then $\gcd(a,b) = \gcd(a,c)$.
(e) We have $\gcd(a,b) = \gcd(a,\ ua+b)$ for any $a, b, u \in \mathbb{Z}$.
(f) We have $\gcd(a,b) = \gcd(a,\ b\%a)$ for any $a, b \in \mathbb{Z}$ with $a > 0$.
(g) We have $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$ for any $a, b \in \mathbb{Z}$.
(h) We have $\gcd(-a,b) = \gcd(a,-b) = \gcd(a,b)$ for any $a, b \in \mathbb{Z}$.
(i) If $a, b \in \mathbb{Z}$ satisfy $a \mid b$, then $\gcd(a,b) = |a|$.

Proof. **(a)** If $\gcd(a,b)$ was negative, then $-\gcd(a,b)$ would be a larger common divisor of a and b, so that $\gcd(a,b)$ would not be the greatest. Thus, $\gcd(a,b)$ must be nonnegative.

(b) Every integer is a divisor of 0. Thus, the common divisors of a and 0 are just the divisors of a. The largest of them is $|a|$ (unless $a = 0$, in which everything is clear anyway). So $\gcd(a,0) = \gcd(0,a) = |a|$.

(c) Obvious.

(d) Let $a, b, c \in \mathbb{Z}$ satisfy $b \equiv c \bmod a$. Assume that $a \neq 0$ (because in the case $a = 0$, the congruence $b \equiv c \bmod a$ becomes $b = c$, which makes the claim obvious).

We must prove that $\gcd(a,b) = \gcd(a,c)$.

Even better, we claim that the common divisors of a and b are precisely the common divisors of a and c. To prove this, we must show the following:

> *Claim 1:* Each common divisor of a and b is a common divisor of a and c.

> *Claim 2:* Each common divisor of a and c is a common divisor of a and b.

Actually, Claim 2 is just Claim 1 with the roles of b and c interchanged. Since the relation $b \equiv c \bmod a$ is symmetric in b and c, the two claims will have analogous proofs. Thus, we will only show the proof of Claim 1.

Proof of Claim 1. Let d be a common divisor of a and b. We must show that d is a common divisor of a and c. By definition of d, we have $d \mid a$ and $d \mid b$, so that $b = dy$ for some integers x and y. But $b \equiv c \bmod a$; this means that $a \mid b - c$. Hence, $d \mid a \mid b - c$, meaning that $b - c = dz$ for some integer z. Hence,

$$c = \underbrace{b}_{=dy} - dz = dy - dz = d\left(y - z\right),$$

so that $d \mid c$. Combining $d \mid a$ with $d \mid c$, we see that d is a common divisor of a and c. Claim 1 is proved. □

Proof of Claim 2. Same as for Claim 1, but with the roles of b and c swapped. □

So $\gcd\left(a, b\right) = \gcd\left(a, c\right)$ is proved. This was part **(d)** of the proposition.

(e) This follows by applying part **(d)** to $c = ua + b$, which is allowed because $b \equiv ua + b \bmod a$.

(f) This follows by applying part **(d)** to $c = b\%a$, which is allowed because $b\%a \equiv b \bmod a$.

(g) If $a = b = 0$, then this is clear. Otherwise, this is just saying that $\gcd\left(a, b\right)$ is a common divisor of a and b, but this again is clear.

(h) The divisors of $-a$ are the divisors of a. The divisors of $-b$ are the divisors of b.

(i) Since $a \mid b$, every divisor of a is a divisor of b. Thus, the common divisors of a and b are just the divisors of a. The largest of them is $\left|a\right|$. □

Corollary 3.4.4 (Euclidean recursion for the gcd)**.** Let $a \in \mathbb{Z}$, and let b be a positive integer. Then,

$$\gcd\left(a, b\right) = \gcd\left(b,\ a\%b\right).$$

Proof. We use the preceding proposition:

$$\begin{aligned}\gcd\left(a, b\right) &= \gcd\left(b, a\right) \\ &= \gcd\left(b,\ a\%b\right) \qquad \left(\text{by part } \textbf{(f)}\text{, with } a \text{ and } b \text{ swapped}\right).\end{aligned}$$

□

3.4.3. The Euclidean algorithm

By applying this corollary repeatedly, we can compute gcds rather quickly:

$$\begin{aligned}
\gcd(93,\ 18) &= \gcd(18,\ 93\%18) && \text{(by the corollary)} \\
&= \gcd(18,\ 3) \\
&= \gcd(3,\ 18\%3) && \text{(by the corollary again)} \\
&= \gcd(3,\ 0) = |3| && \text{(by } \gcd(a,0) = |a|\text{)} \\
&= 3
\end{aligned}$$

and

$$\begin{aligned}
\gcd(1432,\ 739) &= \gcd(739,\ 1432\%739) \\
&= \gcd(739,\ 693) \\
&= \gcd(693,\ 739\%693) \\
&= \gcd(693,\ 46) \\
&= \gcd(46,\ 693\%46) \\
&= \gcd(46,\ 3) \\
&= \gcd(3,\ 46\%3) \\
&= \gcd(3,\ 1) \\
&= \gcd(1,\ 3\%1) \\
&= \gcd(1,\ 0) = |1| = 1.
\end{aligned}$$

These two computations are instances of a general algorithm for computing $\gcd(a,b)$ for any numbers $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. This algorithm proceeds as follows:

- If $b = 0$, then the gcd is $|a|$.
- Otherwise, replace a and b by b and $a\%b$, and recurse (i.e., apply the algorithm to b and $a\%b$ instead of a and b).

Python code:

```
def gcd(a, b): # for b nonnegative
    if b == 0:
        return abs(a) # this is the absolute value of a.
    return gcd(b, a%b)
```

This algorithm is called the **Euclidean algorithm**. Let us convince ourselves that it really terminates (rather than getting stuck in an infinite loop):

Proposition 3.4.5. Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then, the Euclidean algorithm terminates after at most b steps.

Proof. Let b_0 be the initial value of b (at the start of the algorithm).

In each step of the algorithm, the second argument b gets replaced by $a\%b$, which is a number that is smaller than b by at least 1 (since $a\%b \in \{0, 1, \ldots, b-1\}$, so $a\%b \leq b-1$). So the second argument decreases by at least 1 at each step. This cannot go on forever, since it stays nonnegative throughout the algorithm. In fact, this cannot go on for more than b_0 steps, because if it goes on for k steps, then the second argument must be at most $b_0 - k$ after these k steps, and this would be negative if $k > b_0$. So the algorithm must terminate after at most b_0 steps. □

Actually, the proposition greatly overestimates how long the algorithm lasts. In truth, it terminates after at most $\log_2(ab) + 2$ many steps (if a and b are positive). (See the notes for a sketch of the proof.)

The Euclidean algorithm can be easily adapted to negative values of b by recalling that $\gcd(a, -b) = \gcd(a, b)$. Thus the above code becomes:

```
def gcd(a, b): # for b arbitrary
    b = abs(b) # make b nonnegative
    if b == 0:
        return abs(a) # this is the absolute value of a.
    return gcd(b, a%b)
```

The speediness of this algorithm is a big reason why gcds are so useful.

3.4.4. Bezout's theorem and the extended Euclidean algorithm

The Euclidean algorithm can be adapted to not just compute $\gcd(a, b)$ but also to express $\gcd(a, b)$ as an "integer linear combination" of a and b (that is, as a multiple of a plus a multiple of b). This allows us to prove the following theorem:

Theorem 3.4.6 (Bezout's theorem for integers)**.** Let a and b be two integers. Then, there exist two integers x and y such that

$$\gcd(a, b) = xa + yb.$$

In other words, $\gcd(a, b)$ cents can be paid with a-cent coins and b-cent coins, if we are allowed to get change.

Before we prove this, let us give a name to want we want to construct:

Definition 3.4.7. Let a and b be two integers. Then, a **Bezout pair** for (a,b) means a pair (x,y) of integers such that $\gcd(a,b) = xa+yb$.

For instance, a Bezout pair for $(4,7)$ is a pair (x,y) of integers such that $\gcd(4,7) = 4x+7y$, that is, $1 = 4x+7y$. One such pair is $(2,-1)$, since $4\cdot 2 + 7\cdot(-1) = 1$. Another such pair is $(-5,3)$, since $4\cdot(-5)+7\cdot 3 = 1$. A Bezout pair is never unique, since any Bezout pair (x,y) gives rise to other Bezout pairs $(x-b, y+a)$, $(x-2b, y+2a)$, ...

So Bezout's theorem is saying that for any two integers a and b, there is at least one Bezout pair for (a,b).

How can we prove this? We can try strong induction, using

$$\gcd(a,b) = \gcd(a-b,\ b) \qquad \text{or alternatively}$$
$$\gcd(a,b) = \gcd(a\%b,\ b)$$

to reduce our situation to one with a "smaller" pair (a,b). But we need to be careful: Induction (of any kind) requires a lower bound, such as $b \geq 0$, whereas our a and b are arbitrary integers. Also, we need to make sure that $a-b$ is nonnegative, or $a\%b$ is actually smaller than a, or other issues like this. But all in all, the idea works. Here is how.

We begin with the case $b \geq 0$:

Lemma 3.4.8 (restricted Bezout's theorem)**.** Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then, there exists a Bezout pair for (a,b).

Proof. We shall use strong induction on b. Here, we do not fix a. So the statement that we will be proving for all $b \in \mathbb{N}$ is

$$P(b) := (\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a,b)).$$

Our goal is to prove this statement $P(b)$ for all $b \in \mathbb{N}$. We do this by strong induction on b:

Base case: Let us prove $P(0)$. In other words, let us find a Bezout pair for $(a,0)$ for each $a \in \mathbb{Z}$. This must be a pair (x,y) of integers satisfying

$$xa + y\cdot 0 = \gcd(a,0) = |a|.$$

In other words, we need an integer x such that $xa = |a|$. But this is easy: Take $x = 1$ if $a \geq 0$ and $x = -1$ if $a < 0$. So the Bezout pair $(1,0)$ or $(-1,0)$ works.

Induction step: Fix a positive integer b. We must prove the implication

$$(P(0) \text{ AND } P(1) \text{ AND } P(2) \text{ AND } \cdots \text{ AND } P(b-1)) \Longrightarrow P(b).$$

So we assume (as IH) that $P(0)$ AND $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(b-1)$ hold. In other words, we assume that

$$(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a,0)) \text{ and}$$
$$(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a,1)) \text{ and}$$
$$\cdots \text{ and}$$
$$(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a,b-1)).$$

In other words, we assume that for each $a \in \mathbb{Z}$ and each $d \in \{0, 1, \ldots, b-1\}$, there exists a Bezout pair for (a, d).

Our goal is to prove $P(b)$. In other words, we must prove that for each $a \in \mathbb{Z}$, there is a Bezout pair for (a, b).

So fix $a \in \mathbb{Z}$. The Euclidean recursion yields

$$\gcd(a, b) = \gcd(b,\ a\%b).$$

However, $a\%b \in \{0, 1, \ldots, b-1\}$. So our IH yields that there exists a Bezout pair for $(b,\ a\%b)$. Let (u, v) be this Bezout pair. Thus, u and v are integers, and

$$\gcd(b,\ a\%b) = ub + v(a\%b).$$

In view of the above Euclidean recursion, we can rewrite this equation as

$$\begin{aligned}\gcd(a, b) &= ub + v \underbrace{(a\%b)}_{\substack{=a-qb \\ \text{for } q=a//b}} = ub + v(a - qb) \\ &= ub + va - vqb = va + (u - vq)\, b.\end{aligned}$$

This shows that $(v,\ u - vq)$ is a Bezout pair for (a, b). So such a Bezout pair exists, and this completes the induction step. So the lemma is proved by strong induction. □

This inductive proof contains a recursive algorithm for finding a Bezout pair for (a, b) whenever $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Written in Python, it looks as follows:

```
def bezout_pair(a, b): # for b nonnegative
    if b == 0:
        if a >= 0:
            return (1, 0)
        else:
            return (-1, 0)
    (u, v) = bezout_pair(b, a%b)
    q = a // b
    return (v, u - v * q)
```

This algorithm is called the **extended Euclidean algorithm**.

Having proved the lemma (which is saying that a Bezout pair for (a, b) exists whenever $b \in \mathbb{N}$), we can now easily derive Bezout's theorem in the general case (which allows $b < 0$):

Proof of Bezout's theorem. We are in one of two cases:

Case 1: We have $b \geq 0$.

Case 2: We have $b < 0$.

We need to show that there exists a Bezout pair for (a, b).

In Case 1, we have $b \in \mathbb{N}$, so that this claim follows from the lemma.

Now consider Case 2. Here, $b < 0$. Thus, $-b > 0$, so that $-b \in \mathbb{N}$, and therefore we can apply the lemma to $-b$ instead of b. We conclude that there exists a Bezout pair for $(a, -b)$. That is, there exists a pair (u, v) of integers such that $ua + v(-b) = \gcd(a, -b) = \gcd(a, b)$. So

$$\gcd(a, b) = ua + v(-b) = ua + (-v)b.$$

This shows that $(u, -v)$ is a Bezout pair for (a, b). Hence, such a Bezout pair exists, and we are done in Case 2. □

3.4.5. The universal property of the gcd

Bezout's theorem is helpful for proving properties of gcds. Here is the most important one, which I call the **universal property of the gcd**:

Theorem 3.4.9 (universal property of the gcd)**.** Let $a, b, m \in \mathbb{Z}$. Then, we have the equivalence

$$(m \mid a \text{ and } m \mid b) \iff (m \mid \gcd(a, b)).$$

In other words, the common divisors of a and b are precisely the divisors of $\gcd(a, b)$. In other words, $\gcd(a, b)$ is not just the greatest of all common divisors of a and b (at least when a and b are not both 0), but is also divisible by them all.

Proof. We must prove the implications

$$(m \mid a \text{ and } m \mid b) \Longrightarrow (m \mid \gcd(a, b))$$

and

$$(m \mid a \text{ and } m \mid b) \Longleftarrow (m \mid \gcd(a, b)).$$

I will just refer to them as "$\Longrightarrow$" and "$\Longleftarrow$".

The "$\Longleftarrow$" implication is easy: If $m \mid \gcd(a, b)$, then $m \mid \gcd(a, b) \mid a$ (by transitivity of divisibility) and likewise $m \mid b$.

For the "$\Longrightarrow$" implication, we assume that $m \mid a$ and $m \mid b$. We must show that $m \mid \gcd(a, b)$.

Bezout's theorem tells us that $\gcd(a, b) = xa + yb$ for two integers x and y. But both xa and yb are multiples of m (since $m \mid a \mid xa$ and $m \mid b \mid yb$), so that $xa + yb$ is a sum of two multiples of m and thus itself a multiple of m. Hence, $m \mid xa + yb = \gcd(a, b)$. This proves the "$\Longrightarrow$" implication. □

Exercise 3.4.1. If $a_1 \mid b_1$ and $a_2 \mid b_2$, then $\gcd(a_1, a_2) \mid \gcd(b_1, b_2)$.

3.4.6. Factoring out a common factor from a gcd

Theorem 3.4.10 (factoring-out theorem)**.** Let $s, a, b \in \mathbb{Z}$. Then,

$$\gcd(sa, sb) = |s| \cdot \gcd(a, b).$$

For instance, $\gcd(2000,\ 3000) = 1000 \cdot \gcd(2, 3) = 1000$.

Proof of the theorem. Let

$$g = \gcd(a, b) \qquad \text{and} \qquad h = \gcd(sa, sb).$$

We must show that $h = |s| \cdot g$. Since g and h are nonnegative, we can move them into absolute-value brackets: $h = |h|$ and $|s| \cdot g = |sg|$.

So we must prove that $|h| = |sg|$. By what we know about divisibility, it suffices to show that $h \mid sg$ and $sg \mid h$.

- *Proof of $sg \mid h$:* We have $g = \gcd(a, b) \mid a$. Multiplying both sides by s, we obtain $sg \mid sa$. Similarly, $sg \mid sb$. Thus, sg divides both sa and sb, and thus divides $\gcd(sa, sb)$ (by the universal property of the gcd). In other words, sg divides h.
- *Proof of $h \mid sg$:* In the notes, I give two proofs, but here I will only give one.

  We have $h = \gcd(sa, sb) \mid sa$ and likewise $h \mid sb$.

  Bezout's theorem tells us that $\gcd(a, b) = xa + yb$ for two integers x and y. So $g = \gcd(a, b) = xa + yb$. Hence,

$$sg = s(xa + yb) = sxa + syb = x \underbrace{sa}_{\text{a multiple of } h} + y \underbrace{sb}_{\text{a multiple of } h}$$
$$= (\text{a sum of two multiples of } h) = (\text{a multiple of } h).$$

  In other words, $h \mid sg$.

So both $sg \mid h$ and $h \mid sg$ are proved, and we are done. □

One use of gcds is to reduce fractions:

$$\frac{24}{33} = \frac{24/\gcd(24, 33)}{33/\gcd(24, 33)} = \frac{8}{11}.$$

Any time you have a fraction $\frac{a}{b}$ of two integers a and b (with $b \neq 0$), you can cancel $\gcd(a,b)$ from the numerator and denominator, and you obtain a fraction $\frac{a/\gcd(a,b)}{b/\gcd(a,b)}$ that is **reduced** (meaning that its numerator and denominator have gcd $= 1$). The reason for this is that the previous theorem guarantees us that

$$\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1.$$

3.5. Coprime integers

3.5.1. Definition and examples

As this example suggests, gcds are at their most useful when they equal 1. This is known as "coprimality":

Definition 3.5.1. Two integers a and b are said to be **coprime** (or **relatively prime**) if $\gcd(a,b) = 1$.

Remark 3.5.2. This is a symmetric relation, since $\gcd(a,b) = \gcd(b,a)$.

Example 3.5.3. (a) An integer n is coprime to 2 if and only if n is odd. Indeed, if n is even, then $\gcd(n,2) = 2$. If n is odd, then $\gcd(n,2) = 1$.

(b) An integer n is coprime to 3 if and only if $3 \nmid n$.

(c) An integer n is coprime to 4 if and only if n is odd (same answer as for "coprime to 2"). Actually, for any n, we have

$$\gcd(n,4) = \begin{cases} 4, & \text{if } 4 \mid n; \\ 2, & \text{if } 2 \mid n \text{ but } 4 \nmid n; \\ 1, & \text{if } 2 \nmid n. \end{cases}$$

(d) An integer n is coprime to 5 if and only if $5 \nmid n$.

(e) An integer n is coprime to 6 if and only if neither 2 nor 3 divides n.

Informally, I think of coprimality as some kind of number-theoretical "unrelatedness" or "independence" or "orthogonality" or "noninterference" relation.

3.5.2. Three theorems about coprimality

We will now prove three useful properties of coprime integers. The first one:

Theorem 3.5.4 (coprime divisors theorem)**.** Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid c$ and $b \mid c$. Assume that a and b are coprime. Then, $ab \mid c$.

For example, if $2 \mid c$ and $3 \mid c$, then $6 \mid c$ (because 2 and 3 are coprime).

For another example, if $4 \mid c$ and $15 \mid c$, then $60 \mid c$ (because 4 and 15 are coprime).

For a non-example, we have $4 \mid 12$ and $6 \mid 12$ but not $4 \cdot 6 \mid 12$, and this is fine, since 4 and 6 are not coprime.

Proof of theorem. We have $ab \mid ac$ (since $b \mid c$) and $ba \mid bc$ (since $a \mid c$). Hence, $ab = ba$ is a common divisor of ac and bc. By the universal property of the gcd, this yields

$$\begin{aligned} ab \mid \gcd(ac, bc) &= \gcd(ca, cb) \\ &= |c| \cdot \underbrace{\gcd(a, b)}_{\substack{=1 \\ \text{(since } a \text{ and } b \text{ are coprime)}}} && \text{(by the factoring-out theorem)} \\ &= |c| \mid c, \end{aligned}$$

qed. □

Our next property of coprime integers is the following:

Theorem 3.5.5 (coprime removal theorem)**.** Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid bc$. Assume that a is coprime to b. Then, $a \mid c$.

Proof. The number a is a common divisor of bc and ac. Hence, by the universal property,

$$\begin{aligned} a \mid \gcd(bc, ac) &= \gcd(ac, bc) = \gcd(ca, cb) \\ &= |c| \cdot \underbrace{\gcd(a, b)}_{=1} = |c| \mid c, \end{aligned}$$

qed. □

Finally, our third property:

Theorem 3.5.6 (coprime product theorem)**.** Let $a, b, c \in \mathbb{Z}$. Assume that each of a and b is coprime to c. Then, ab is also coprime to c.

Proof. Let $g = \gcd(ab, c)$. We must show that $g = 1$.

But g is a common divisor of ab and ac (since $g \mid c \mid ac$). Hence, by the universal property,

$$\begin{aligned} g \mid \gcd(ab, ac) &= |a| \cdot \underbrace{\gcd(b, c)}_{\substack{=1 \\ \text{(since } b \text{ is coprime to } c\text{)}}} && \text{(by the factoring-out theorem)} \\ &\mid |a| \mid a. \end{aligned}$$

Combining this with $g \mid c$, we see that g is a common divisor of a and c. Hence, by the universal property again,

$$g \mid \gcd(a, c) = 1 \qquad (\text{since } a \text{ is coprime to } c).$$

Since g is nonnegative, this entails $g = 1$, qed. □

Note that the first two of these theorems have versions for non-coprime integers, which are a bit more complicated. See the notes (Theorems 3.5.10 and 3.5.11).

3.5.3. Reducing a fraction

Theorem 3.5.7. Let a and b be two integers that are not both 0. Let $g = \gcd(a, b)$. Then, the integers $\frac{a}{g}$ and $\frac{b}{g}$ are coprime.

Proof. Let $h = \gcd\left(\frac{a}{g}, \frac{b}{g}\right)$. Then, gh is a common divisor of a and b (since $h \mid \frac{a}{g}$ means that $gh \mid a$, and likewise we get $gh \mid b$), and therefore we have $gh \leq g$ since g is the greatest common divisor of a and b. Since g is positive, this entails $h \leq 1$ and thus $h = 1$ (since h is a gcd of two integers that are not both 0). In other words, $\frac{a}{g}$ and $\frac{b}{g}$ are coprime. □

As an application of this theorem, we can bring any fraction into reduced form. We say that a fraction $\frac{u}{v}$ of two integers u and v is in **reduced form** if u and v are coprime. Now, the theorem tells us that we can transform any fraction $\frac{a}{b}$ (with $b \neq 0$) into reduced form by cancelling $g = \gcd(a, b)$ from numerator and denominator, since it guarantees us that $\frac{a}{g}$ and $\frac{b}{g}$ are coprime. For instance, $\frac{12}{21} = \frac{12/3}{21/3} = \frac{4}{7}$.

3.6. Prime numbers

3.6.1. Definition

Definition 3.6.1. An integer $n > 1$ is said to be **prime** (or **a prime**) if the only positive divisors of n are 1 and n.

The first few primes (= prime numbers) are

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43.$$

It can be shown that there are infinitely many primes.

3.6.2. The friend-or-foe lemma

The first property of primes that we will show is a crucial result I call the **friend-or-foe lemma**:

Lemma 3.6.2 (friend-or-foe lemma)**.** Let p be a prime. Let $n \in \mathbb{Z}$. Then, n is either divisible by p or coprime to p.

Proof. The number p is prime, so its only positive divisors are 1 and p. But $\gcd(n,p)$ is a positive divisor of p. So $\gcd(n,p)$ must be 1 or p.

If $\gcd(n,p) = 1$, then n is coprime to p.

If $\gcd(n,p) = p$, then n is divisible by p (since $p = \gcd(n,p) \mid n$). □

In contrast, the lemma would not be true for $p = 4$: For instance, the number $n = 2$ is neither divisible by 4 nor coprime to 4.

Similarly, for $p = 6$, the number $n = 2$ is neither divisible by 6 nor coprime to 6.

3.6.3. Binomial coefficients and primes

Looking at Pascal's triangle, we might notice that for any prime p, the numbers in the p-th row except for the two 1's at its two ends are all divisible by p. For instance, $\binom{7}{1}$, $\binom{7}{2}$, $\ldots$, $\binom{7}{6}$ are divisible by 7. This pattern holds indeed for all the primes:

Theorem 3.6.3. Let p be a prime. Let $k \in \{1,2,\ldots,p-1\}$. Then, $p \mid \binom{p}{k}$.

Proof. Homework set #3 exercise 5 **(a)** yields

$$k\binom{p}{k} = p\underbrace{\binom{p-1}{k-1}}_{\text{an integer}}.$$

Thus, $p \mid k\binom{p}{k}$.

However, $p \nmid k$ (since $k \in \{1,2,\ldots,p-1\}$). But the friend-or-foe lemma shows that k is either divisible by p or coprime to p. Since $p \nmid k$, we thus conclude that k is coprime to p. By the coprime removal theorem, we can thus obtain $p \mid \binom{p}{k}$ from $p \mid k\binom{p}{k}$. □

3.6.4. Fermat's Little Theorem

It is easy to see that every integer a satisfies $a^2 \equiv a \bmod 2$. Indeed, this is saying that $2 \mid a^2 - a = a(a-1)$, but clearly one of a and $a-1$ is even.

It is also easy to see that every integer a satisfies $a^3 \equiv a \bmod 3$. Indeed, this is saying that $3 \mid a^3 - a = (a+1)a(a-1)$, but clearly one of $a+1$ and a and $a-1$ is divisible by 3.

It is less easy to see that every integer a satisfies $a^5 \equiv a \bmod 5$. This can be proved by brute force, through checking all possible cases $a \equiv 0 \bmod 5$ and $a \equiv 1 \bmod 5$ and $a \equiv 2 \bmod 5$ and $a \equiv 3 \bmod 5$ and $a \equiv 4 \bmod 5$.

It is even less easy to see that every integer a satisfies $a^7 \equiv a \bmod 7$.

I claim that this all generalizes:

Theorem 3.6.4 (Fermat's Little Theorem)**.** Let p be a prime. Let $a \in \mathbb{Z}$. Then,

$$a^p \equiv a \bmod p.$$

Note that this is usually false when p is not a prime. For example, $a^4 \not\equiv a \bmod 4$ when $a = 2$. There are some weird non-prime numbers p for which $a^p \equiv a \bmod p$ is still always true, but they are rare (the smallest such p are 1, 561, 1105, 1729, 2465). They are called **Carmichael numbers**.

Proof of the theorem. We induct on a, in order to cover the cases $a \geq 0$.

Base case: We have $0^p \equiv 0 \bmod p$, since $p > 0$ entails $0^p = 0$.

Induction step: Let $a \in \mathbb{N}$. Assume (as IH) that $a^p \equiv a \bmod p$. We must prove that $(a+1)^p \equiv a+1 \bmod p$.

The binomial theorem yields

$$\begin{aligned}
(a+1)^p &= \sum_{k=0}^{p} \binom{p}{k} a^k \underbrace{1^{p-k}}_{=1} \\
&= \sum_{k=0}^{p} \binom{p}{k} a^k \\
&= \underbrace{\binom{p}{0}}_{=1} \underbrace{a^0}_{=1} + \underbrace{\sum_{k=1}^{p-1} \binom{p}{k} a^k}_{\substack{\text{This is a sum of multiples of } p \\ \text{(since } p \mid \binom{p}{k} \text{ by the previous theorem),} \\ \text{so it is } \equiv 0 \bmod p}} + \underbrace{\binom{p}{p}}_{=1} \underbrace{a^p}_{\equiv a \bmod p} \\
&\equiv 1 + 0 + a = a + 1 \bmod p.
\end{aligned}$$

This completes the induction step, and thus proves the theorem... for all $a \in \mathbb{N}$.

It remains to prove it for negative a.

There is a simple way to reduce the negative-a case to the $a \in \mathbb{N}$ case:

Let a be negative. Then, we pick a nonnegative b such that $b \equiv a \bmod p$. (For example, $b := a\%p$.) Thus, by the part of the theorem that we already proved, we have $b^p \equiv b \bmod p$. But $b \equiv a \bmod p$, so that $b^p \equiv a^p \bmod p$. Hence,

$$a^p \equiv b^p \equiv b \equiv a \bmod p,$$

and we are done. (Essentially, we have used b as a "nonnegative proxy" for a.) □

3.6.5. Prime divisor separation theorem

You can think of primes as "inseparable" positive integers: They cannot be written as products of two smaller positive integers.

One useful consequence of this "inseparability" is that if a prime p divides a product ab of two integers, then p must divide one of the factors a and b. But this is not a proof, though the claim is correct. So let us prove it:

Theorem 3.6.5 (prime divisor separation theorem)**.** Let p be a prime. Let $a, b \in \mathbb{Z}$ be such that $p \mid ab$. Then, $p \mid a$ or $p \mid b$.

Proof. By the friend-or-foe lemma, a is either divisible by p or coprime to p. In the former case, we are done (we get $p \mid a$). Remains to consider the latter case. So a is coprime to p. Thus, by the coprime removal theorem, we can transform $p \mid ab$ into $p \mid b$, and we are also done. □

Corollary 3.6.6 (prime divisor separation theorem for k factors)**.** Let p be a prime. Let $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ be such that $p \mid a_1 a_2 \cdots a_k$. Then, $p \mid a_i$ for some $i \in \{1, 2, \ldots, k\}$.

(In other words: If a prime p divides a product of some integers, then p divides at least one of its factors.)

Proof. Induct on k, using $a_1 a_2 \cdots a_k = (a_1 a_2 \cdots a_{k-1})\, a_k$ and the theorem above.

(For the base case $k = 0$, use $p \nmid 1$.) □

3.6.6. p-valuations: definition

We will need a simple lemma:

Lemma 3.6.7. Let p be a prime (or just an integer > 1). Let n be a nonzero integer. Then, there exists a largest $m \in \mathbb{N}$ such that $p^m \mid n$.

Proof. First of all, there exists at least one $m \in \mathbb{N}$ such that $p^m \mid n$, namely $m = 0$.

But the set of such m is finite, since the sequence of powers of p increases unboundedly: $p^0 < p^1 < p^2 < \cdots$ and thus eventually outgrows $|n|$, but we must have $p^m \leq |n|$ in order to have $p^m \mid n$. □

This lemma allows us to make the following definition:

Definition 3.6.8. Let p be a prime.

(a) Let n be a nonzero integer. Then, $v_p(n)$ shall denote the largest $m \in \mathbb{N}$ such that $p^m \mid n$. (This is well-defined by the lemma above.)

This number $v_p(n)$ is called the **p-valuation** (or **p-adic valuation**) of n.

(b) In order to not leave $v_p(0)$ undefined, we set $v_p(0) := \infty$. (The symbol ∞ behaves by the rules $\infty + k = \infty$ and $\infty + \infty = \infty$ and $\infty > k$ for all $k \in \mathbb{Z}$. Don't subtract ∞ from anything.)

Here are some examples:

$$v_3(99) = 2 \qquad \left(\text{since } 3^2 \mid 99 \text{ but } 3^3 \nmid 99\right);$$
$$v_3(98) = 0 \qquad \left(\text{since } 3^0 \mid 98 \text{ but } 3^1 \nmid 98\right);$$
$$v_3(96) = 1 \qquad \left(\text{since } 3^1 \mid 96 \text{ but } 3^2 \nmid 96\right);$$
$$v_3(0) = \infty.$$

We can restate the definition of $v_p(n)$ in two other ways: If p is a prime and n is a positive integer, then:

- $v_p(n)$ is the number of times you can divide n by p without getting a non-integer;
- $v_p(n)$ is the number of zeroes at the end of the base-p representation of n.

For example, the number 344 is 101011000 in base 2, so we get $v_2(344) = 3$.

So far, we didn't really need p to be a prime, as the definition works for any integer $p > 1$. Soon we will see how the primality of p makes p-valuations behave nicer than otherwise.

3.6.7. p-valuations: basic properties

I will only outline the proofs; see the notes for details.

Lemma 3.6.9. Let p be a prime. Let $i \in \mathbb{N}$ and $n \in \mathbb{Z}$. Then, $p^i \mid n$ if and only if $v_p(n) \geq i$.

Proof. Both cases $n = 0$ and $n \neq 0$ are easy. □

Theorem 3.6.10 (basic properties of p-valuations)**.** Let p be a prime. Then:
(a) We have $v_p(ab) = v_p(a) + v_p(b)$ for any $a, b \in \mathbb{Z}$.
(b) We have $v_p(a+b) \geq \min\left\{v_p(a),\ v_p(b)\right\}$ for any $a, b \in \mathbb{Z}$.
(c) We have $v_p(1) = 0$.
(d) We have $v_p(p) = 1$.
(e) We have $v_p(q) = 0$ for any prime $q \neq p$.

Proof. Parts **(b)**–**(e)** are mostly trivial. (For part **(b)**, keep in mind that ∞ is larger than all normal integers, so $\min\{k, \infty\} = \min\{\infty, k\} = k$.)

For part **(a)**, fix $a, b \in \mathbb{Z}$. WLOG assume that neither a nor b is 0, since the other case is obvious (it boils down to $\infty = \infty + k$). In this case, write

$$\begin{aligned} a &= p^{v_p(a)} x \qquad \text{with } p \nmid x \qquad \text{and} \\ b &= p^{v_p(b)} y \qquad \text{with } p \nmid y. \end{aligned}$$

Then, by the friend-or-foe lemma, x and y are coprime to p. Hence, $p \nmid xy$ (since $p \mid xy$ would yield $p \mid y$ by the coprime removal theorem, and this would contradict $p \nmid y$). But

$$ab = p^{v_p(a)} x p^{v_p(b)} y = p^{v_p(a)+v_p(b)} \underbrace{xy}_{\text{not divisible by } p}.$$

Hence, $v_p(ab) = v_p(a) + v_p(b)$, qed. □

Corollary 3.6.11. Let p be a prime. Then,

$$v_p(a_1 a_2 \cdots a_k) = v_p(a_1) + v_p(a_2) + \cdots + v_p(a_k)$$

for any k integers $a_1, a_2, \ldots, a_k$.

Proof. Induct on k, using the previous theorem. □

3.6.8. Back to Hanoi

Let us take a closer look at 2-valuations. The sequence

$$\begin{aligned} &(v_2(1),\ v_2(2),\ v_2(3),\ v_2(4),\ v_2(5),\ \ldots) \\ &= (0,\ 1,\ 0,\ 2,\ 0,\ 1,\ 0,\ 3,\ 0,\ 1,\ 0,\ 2,\ 0,\ 1,\ 0,\ 4,\ \ldots) \end{aligned}$$

is called the **ruler sequence**. It appears in many unrelated places, in particular:

Proposition 3.6.12. Let $n \in \mathbb{N}$. Recall the strategy we proposed for solving the Tower of Hanoi puzzle with n disks.

For each $k \in \{1, 2, \ldots, 2^n - 1\}$, the k-th move of this strategy moves the $(v_2(k)+1)$-th smallest disk.

Proof. See the notes. (Essentially, induction on n.) □

3.6.9. The p-valuation of $n!$

How many zeroes does the number 50! end with? What about other bases?

For prime bases, the following formula gives an answer:

Theorem 3.6.13. Let p be a prime. Let $n \in \mathbb{N}$. Then,

$$\begin{aligned} v_p(n!) &= \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \\ &= \left(n//p^1\right) + \left(n//p^2\right) + \left(n//p^3\right) + \cdots . \end{aligned}$$

(The infinite sums here make sense because all of their addends except for the first few are 0. For instance, for $p = 2$ and $n = 14$, we have

$$\begin{aligned} &\left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \\ &= \lfloor 7 \rfloor + \lfloor 3.5 \rfloor + \lfloor 1.75 \rfloor + \lfloor 0.875 \rfloor + \lfloor 0.4375 \rfloor + \cdots \\ &= 7 + 3 + 1 + 0 + 0 + 0 + \cdots \\ &= 7 + 3 + 1 = 11. \end{aligned}$$

The same pattern occurs for all n and p: Starting at some k, we have $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$, so we only need to sum the first $k-1$ addends.)

Proof. The two infinite sums

$$\left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \qquad \text{and}$$
$$\left(n//p^1\right) + \left(n//p^2\right) + \left(n//p^3\right) + \cdots$$

are equal, since $\left\lfloor \frac{n}{k} \right\rfloor = n//k$ for every $k > 0$. Moreover, these sums are actually finite sums in disguise, since every sufficiently high k satisfies $p^k > n$ and therefore $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$. (Zeroes do not affect a sum, even if there are infinitely many of them.)

It remains to prove that

$$v_p(n!) = \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots .$$

We can prove this by induction on n.

Base case: This claims that $v_p(0!) = \left\lfloor \frac{0}{p^1} \right\rfloor + \left\lfloor \frac{0}{p^2} \right\rfloor + \left\lfloor \frac{0}{p^3} \right\rfloor + \cdots$. This is just saying $0 = 0$.

Induction step: We proceed from $n-1$ to n. So we fix a positive integer n, and we assume (as IH) that

$$v_p\left((n-1)!\right) = \left\lfloor \frac{n-1}{p^1} \right\rfloor + \left\lfloor \frac{n-1}{p^2} \right\rfloor + \left\lfloor \frac{n-1}{p^3} \right\rfloor + \cdots .$$

We must now prove that

$$v_p\left(n!\right) = \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots .$$

We first compare the LHSs: From $n! = (n-1)! \cdot n$, we see that

$$\begin{aligned} v_p\left(n!\right) &= v_p\left((n-1)! \cdot n\right) \\ &= v_p\left((n-1)!\right) + v_p\left(n\right) \\ &= \left\lfloor \frac{n-1}{p^1} \right\rfloor + \left\lfloor \frac{n-1}{p^2} \right\rfloor + \left\lfloor \frac{n-1}{p^3} \right\rfloor + \cdots + v_p\left(n\right) \end{aligned}$$

by the IH. We must show that this equals

$$\left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots .$$

So let us compare $\left\lfloor \frac{n}{p^i} \right\rfloor$ and $\left\lfloor \frac{n-1}{p^i} \right\rfloor$. By the birthday lemma

$$\begin{aligned} \left\lfloor \frac{n}{d} \right\rfloor &= \left\lfloor \frac{n-1}{d} \right\rfloor + 1 \qquad \text{if } d \mid n; \\ \left\lfloor \frac{n}{d} \right\rfloor &= \left\lfloor \frac{n-1}{d} \right\rfloor \qquad \text{if } d \nmid n \end{aligned}$$

(applied to $d = p^i$), we obtain

$$\begin{aligned} \left\lfloor \frac{n}{p^i} \right\rfloor &= \left\lfloor \frac{n-1}{p^i} \right\rfloor + 1 \qquad \text{if } p^i \mid n; \\ \left\lfloor \frac{n}{p^i} \right\rfloor &= \left\lfloor \frac{n-1}{p^i} \right\rfloor \qquad \text{if } p^i \nmid n. \end{aligned}$$

Thus, for each $i \in \left\{1, 2, \ldots, v_p\left(n\right)\right\}$, we have

$$\left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{n-1}{p^i} \right\rfloor + 1 \qquad \left(\text{since } i \leq v_p\left(n\right) \text{ and so } p^i \mid n\right),$$

whereas for each $i > v_p\left(n\right)$, we have

$$\left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{n-1}{p^i} \right\rfloor \qquad \left(\text{since } i > v_p\left(n\right) \text{ and so } p^i \nmid n\right).$$

Altogether, this means that the addends of the infinite sum

$$\left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

agree with the addends of the infinite sum

$$\left\lfloor \frac{n-1}{p^1} \right\rfloor + \left\lfloor \frac{n-1}{p^2} \right\rfloor + \left\lfloor \frac{n-1}{p^3} \right\rfloor + \cdots$$

except that the first $v_p(n)$ addends have each been increased by 1.

Hence, in total,

$$\begin{aligned}
&\left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \\
&= \left\lfloor \frac{n-1}{p^1} \right\rfloor + \left\lfloor \frac{n-1}{p^2} \right\rfloor + \left\lfloor \frac{n-1}{p^3} \right\rfloor + \cdots \\
&\qquad + \underbrace{1+1+\cdots+1}_{v_p(n) \text{ many}} \\
&= \left\lfloor \frac{n-1}{p^1} \right\rfloor + \left\lfloor \frac{n-1}{p^2} \right\rfloor + \left\lfloor \frac{n-1}{p^3} \right\rfloor + \cdots + v_p(n).
\end{aligned}$$

This is precisely what we needed to prove. So the induction is complete. □

3.6.10. Prime factorization

We are now ready to prove one of the most important properties of primes: the fact that every positive integer can be uniquely decomposed into a product of primes. For instance,

$$200 = 2 \cdot 100 = 2 \cdot 2 \cdot 50 = 2 \cdot 2 \cdot 2 \cdot 25 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5.$$

The word "uniquely" means here that any two ways of decomposing the same number into a product of primes are equal up to reordering the factors. (So $2 \cdot 5 \cdot 2 \cdot 5 \cdot 2$ counts as the same factorization of 200.)

Let us state this fact in full generality. First, we introduce a name for these decompositions:

Definition 3.6.14. Let n be a positive integer. A **prime factorization** of n means a finite list $(p_1, p_2, \ldots, p_k)$ of primes (not necessarily distinct) such that

$$n = p_1 p_2 \cdots p_k.$$

For instance, $(2,2,2,5,5)$ and $(2,5,2,5,2)$ are two prime factorizations of 200. By reordering the factors, we can get other prime factorizations of 200, but this amounts for all of them. Let me state this claim in its general case:

Theorem 3.6.15 (Fundamental Theorem of Arithmetic)**.** Let n be a positive integer. Then:

(a) There exists a prime factorization of n.

(b) This prime factorization is unique up to reordering its entries. In other words, if $(p_1, p_2, \ldots, p_k)$ and $(q_1, q_2, \ldots, q_\ell)$ of n, then $(q_1, q_2, \ldots, q_\ell)$ can be obtained from $(p_1, p_2, \ldots, p_k)$ by reordering the entries.

(c) Let $(p_1, p_2, \ldots, p_k)$ be a prime factorization of n. Let p be any prime. Then, the number of times that p appears in the list $(p_1, p_2, \ldots, p_k)$ (in other words, the number of $i \in \{1, 2, \ldots, k\}$ such that $p_i = p$) is $v_p(n)$.

Proof. **(a)** This was the "Every positive integer is a product of finitely many primes" theorem that we proved long ago using strong induction.

(c) By the definition of a prime factorization, we have $n = p_1 p_2 \cdots p_k$. Hence,

$$\begin{aligned} v_p(n) &= v_p(p_1 p_2 \cdots p_k) \\ &= v_p(p_1) + v_p(p_2) + \cdots + v_p(p_k) \qquad \text{(by the last corollary)}. \end{aligned}$$

But we know that $v_p(p) = 1$, whereas $v_p(q) = 0$ for any prime $q \neq p$. Hence, any addend $v_p(p_i)$ in the above sum will be 1 if $p_i = p$ and 0 otherwise. So the sum has a 1 for each i that satisfies $p_i = p$, and a 0 for each remaining i. Thus, the value of this sum is the number of 1's, i.e., the number of i's that satisfy $p_i = p$. So we conclude that

$$\begin{aligned} v_p(n) &= (\text{the number of } i \in \{1, 2, \ldots, k\} \text{ that satisfy } p_i = p) \\ &= (\text{the number of times } p \text{ appears in } (p_1, p_2, \ldots, p_k)). \end{aligned}$$

This proves part **(c)**.

(b) Let $(p_1, p_2, \ldots, p_k)$ and $(q_1, q_2, \ldots, q_\ell)$ be two prime factorizations of n. Then, for every prime p, part **(c)** yields

$$(\text{the number of times } p \text{ appears in } (p_1, p_2, \ldots, p_k)) = v_p(n),$$

and similarly

$$(\text{the number of times } p \text{ appears in } (q_1, q_2, \ldots, q_\ell)) = v_p(n).$$

So the prime p appears equally often in $(p_1, p_2, \ldots, p_k)$ as it does in $(q_1, q_2, \ldots, q_\ell)$. And this is true for any prime p. So the two tuples $(p_1, p_2, \ldots, p_k)$ and $(q_1, q_2, \ldots, q_\ell)$ contain the same primes the same number of times. Thus they can only differ in the order of their entries. This proves part **(b)**. □

The Fundamental Theorem of Arithmetic, or rather its proof, gives an algorithm for computing a prime factorization of a positive integer n: Let d be the smallest positive divisor of n. Then, factor n/d into a primes, and append d to that factorization. This is what we did with 200 above.

Note that the positive integer 1 has a trivial prime factorization: the empty tuple $()$. What does not have prime factorizations are 0 and negative integers.

3.7. Least common multiples

Least common multiples (lcm) are the greatest common divisors' older siblings:

Definition 3.7.1. Let a and b be two integers.

(a) The **common multiples** of a and b are the integers that are divisible by a and also by b.

(b) The **least common multiple** (aka the **lowest common multiple**, or the **lcm**) of a and b is defined as follows:

- If a and b are nonzero, then it is the smallest positive common multiple of a and b.
- Otherwise, it is 0.

It is denoted by $\operatorname{lcm}(a,b)$.

For example,

$$\operatorname{lcm}(4,6) = 12; \qquad \operatorname{lcm}(3,4) = 12;$$
$$\operatorname{lcm}(6,8) = 24; \qquad \operatorname{lcm}(2,4) = 4;$$
$$\operatorname{lcm}(0,5) = 0; \qquad \operatorname{lcm}(-2,3) = 6.$$

Note that the lcm of two positive integers is a known concept: When you bring two fractions (of integers) to their lowest common denominator, this lowest common denominator is the lcm of their denominators.

Here are some basic properties of lcms:

Proposition 3.7.2. Let a and b be two integers. Then:

(a) The lcm of a and b exists.

(b) We have $\operatorname{lcm}(a,b) \in \mathbb{N}$.

(c) We have $\operatorname{lcm}(a,b) = \operatorname{lcm}(b,a)$.

(d) We have $a \mid \operatorname{lcm}(a,b)$ and $b \mid \operatorname{lcm}(a,b)$.

(e) We have $\operatorname{lcm}(-a,b) = \operatorname{lcm}(a,-b) = \operatorname{lcm}(a,b)$.

Proof. All of this is easy. For part **(a)**, we observe that $|ab|$ is a positive common multiple of a and b (when a and b are nonzero), so that a positive common multiple exists, and therefore there is a smallest one. □

Here is a counterpart to the universal property of the gcd:

Theorem 3.7.3 (universal property of the lcm)**.** Let $a, b, m \in \mathbb{Z}$. Then, we have the equivalence

$$(a \mid m \text{ and } b \mid m) \iff (\operatorname{lcm}(a,b) \mid m).$$

Proof. $\Longleftarrow$: If $\operatorname{lcm}(a,b) \mid m$, then $a \mid \operatorname{lcm}(a,b) \mid m$ and $b \mid \operatorname{lcm}(a,b) \mid m$.

$\Longrightarrow$: Assume that $a \mid m$ and $b \mid m$. We must show that $\operatorname{lcm}(a,b) \mid m$.

If one of a and b is 0, then this is clear (since $\operatorname{lcm}(a,b)$ is 0 and thus is one of a and b). It remains to handle the case when a and b are nonzero.

In this case, set $\ell = \operatorname{lcm}(a,b)$, and observe that ℓ is defined as the smallest positive common multiple of a and b. Now, divide m by ℓ with remainder (since ℓ is positive). Let q and r be the quotient $m//\ell$ and the remainder $m\%\ell$. Then,

$$q \in \mathbb{Z} \qquad \text{and} \qquad r \in \{0, 1, \ldots, \ell - 1\} \qquad \text{and} \qquad m = q\ell + r.$$

The latter equality yields $r = m - q\ell$. But m and ℓ are multiples of a; thus, $r = m - q\ell$ is also a multiple of a. Similarly, r is a multiple of b. So r is a common multiple of a and b. If r was positive, then r would therefore be $\geq \ell$ (since ℓ is the smallest positive common multiple of a and b), but this would contradict $r \in \{0, 1, \ldots, \ell - 1\}$. So r cannot be positive. Since $r \in \{0, 1, \ldots, \ell - 1\}$. Hence, $r = 0$. So $m\%\ell = r = 0$. This means that m is divisible by $\ell = \operatorname{lcm}(a,b)$. In other words, $\operatorname{lcm}(a,b) \mid m$. □

There are some other properties of lcms that make them useful. Maybe the most important one is the following formula, which allows us to compute $\operatorname{lcm}(a,b)$ from $\gcd(a,b)$:

Theorem 3.7.4. Let a and b be two integers. Then,

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|.$$

Proof. If a or b is 0, then this is easy. Otherwise, the fraction $\dfrac{ab}{\gcd(a,b)}$ is an integer, since $\gcd(a,b) \mid a \mid ab$. Moreover, this fraction is a common multiple of a and b (indeed, $b \mid \dfrac{ab}{\gcd(a,b)}$ boils down to $b \mid \dfrac{ab}{\gcd(a,b)}$, which follows from $1 \mid \dfrac{a}{\gcd(a,b)}$, which is clear since $\gcd(a,b) \mid a$), hence a multiple of $\operatorname{lcm}(a,b)$ (by the universal property of the lcm). This shows that

$$\operatorname{lcm}(a,b) \mid \frac{ab}{\gcd(a,b)},$$

hence

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) \mid ab.$$

On the other hand, to prove

$$ab \mid \gcd(a,b) \cdot \operatorname{lcm}(a,b),$$

it suffices to show that

$$\frac{ab}{\operatorname{lcm}(a,b)} \mid \gcd(a,b),$$

which is because $\dfrac{ab}{\operatorname{lcm}(a,b)}$ is an integer (since ab is a common multiple of a and b, hence divisible by $\operatorname{lcm}(a,b)$ by the universal property) and is a common divisor of a and b (in fact, $\dfrac{ab}{\operatorname{lcm}(a,b)} \mid a$ boils down to $ab \mid a \operatorname{lcm}(a,b)$, which follows from $b \mid \operatorname{lcm}(a,b)$), which means by the universal property of the gcd that $\dfrac{ab}{\operatorname{lcm}(a,b)} \mid \gcd(a,b)$.

So we have shown that

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) \mid ab$$

and

$$ab \mid \gcd(a,b) \cdot \operatorname{lcm}(a,b).$$

Combining these, we obtain

$$|\gcd(a,b) \cdot \operatorname{lcm}(a,b)| = |ab|.$$

In other words,

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|,$$

since gcds and lcms are always nonnegative. □

Both gcds and lcms have easily computable p-valuations:

Theorem 3.7.5. Let p be a prime. Let a and b be two integers. Then,

$$v_p(\gcd(a,b)) = \min\{v_p(a),\ v_p(b)\} \qquad \text{and}$$
$$v_p(\operatorname{lcm}(a,b)) = \max\{v_p(a),\ v_p(b)\}.$$

Proof. See the notes for a reference. □

This theorem provides an easy way to compute gcds and lcms of two integers a and b if you know the prime factorizations of a and b. For larger numbers, however, prime factorizations cannot be computed efficiently (at least not with the methods of today), and so the best way to compute gcds and lcms remains the Euclidean algorithm (that gives you $\gcd(a,b)$, and then you find $\operatorname{lcm}(a,b)$ from $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|$).

3.8. Sylvester's $xa + yb$ theorem (or the Chicken McNugget theorem)

The following is a bit of an aside, but it gives an interesting result that answers a question implicitly posed two chapters ago.

For this whole section, we let a and b be two positive integers.

Definition 3.8.1. **(a)** A **$\mathbb{Z}$-linear combination** of a and b will mean a number of the form

$$xa + yb \qquad \text{with } x, y \in \mathbb{Z}.$$

In other words, it means a number of cents that you can pay with a-cent coins and b-cent coins if you can get change.

(b) An **$\mathbb{N}$-linear combination** of a and b will mean a number of the form

$$xa + yb \qquad \text{with } x, y \in \mathbb{N}.$$

In other words, it means a number of cents that you can pay with a-cent coins and b-cent coins without getting change.

Now, one of our above examples for strong induction tells us that any integer $n \geq 8$ is an $\mathbb{N}$-linear combination of 3 and 5. Moreover, the $\mathbb{N}$-linear combinations of 3 and 5 are

$$0,\ 3,\ 5,\ 6,\ \underbrace{8,\ 9,\ 10,\ \ldots}_{\text{all integers } \geq 8}.$$

One homework problem asked you for $\mathbb{N}$-linear combinations of p and $p+1$.

What about $\mathbb{N}$-linear combinations of a and b in the general case?

We begin by describing the $\mathbb{Z}$-linear combinations:

Proposition 3.8.2. The $\mathbb{Z}$-linear combinations of a and b are exactly the multiples of $\gcd(a, b)$.

Proof. Follows easily from Bezout. See the notes for details. □

Now we move on to the $\mathbb{N}$-linear combinations. The first thing we observe is that all of them are multiples of $\gcd(a, b)$, so we can reduce the problem to smaller numbers by factoring out $\gcd(a, b)$ from both a and b. Namely, the $\mathbb{N}$-linear combinations of a and b are just the $\mathbb{N}$-linear combinations of $\dfrac{a}{\gcd(a, b)}$ and $\dfrac{b}{\gcd(a, b)}$, each multiplied by $\gcd(a, b)$.

So we can restrict ourselves to the case when a and b are coprime.

Another example: The $\mathbb{N}$-linear combinations of 5 and 9 are

$$0,\ 5,\ 9,\ 10,\ 14,\ 15,\ 18,\ 19,\ 20,\ 23,\ 24,\ 25,\ 27,\ 28,\ 29,\ 30,\ \underbrace{32,\ 33,\ 34,\ \ldots}_{\text{all } \geq 32}.$$

Note that every integer $n \geq 32$ is an $\mathbb{N}$-linear combination of 5 and 9. Among the first 32 nonnegative integers $0, 1, \ldots, 31$, exactly half (that is, 16) are $\mathbb{N}$-linear combinations of 5 and 9.

This phenomenon generalizes:

Theorem 3.8.3 (Sylvester's two-coin theorem, or Chicken McNugget theorem)**.** Assume that the positive integers a and b are coprime. Then:

(a) Every number $n > ab - a - b$ is an $\mathbb{N}$-linear combination of a and b.

(b) The number $ab - a - b$ is **not** an $\mathbb{N}$-linear combination of a and b.

(c) Among the first $(a-1)(b-1)$ nonnegative integers $0, 1, \ldots, ab - a - b$, exactly half are $\mathbb{N}$-linear combinations of a and b.

(d) Let $n \in \mathbb{Z}$. Then, exactly one of the two numbers n and $ab - a - b - n$ is an $\mathbb{N}$-linear combination of a and b.

For the proof of this theorem, see the notes. The main idea is to start with **(b)**, which easily yields the "at most one" part of **(d)**; then prove **(d)** using Bezout's theorem and some moving-around of the coefficients.

Much deeper questions arise when you allow three or more denominations of coins, i.e., when you ask for the $\mathbb{N}$-linear combinations of three integers a, b, c (or more than three).

3.9. Digression: An introduction to cryptography

In this short section, we will make a little foray into **cryptography** (aka **cryptology**): the study of ciphers, i.e., methods of encrypting data. This field has millenia worth of history, and is not really a subfield of mathematics, but it involves a lot of mathematics.

We will see an ancient (Roman) as well as a modern (20th century) cipher. Both ciphers are based on elementary number theory, specifically modular arithmetic. The second is still used occasionally, while the former is nowadays only used in puzzles. Many more ciphers have been invented in the meantime; see any text on cryptography (some references are in the notes).

3.9.1. Caesarian ciphers (alphabet rotation)

... (To be filled in) ....

4. An informal introduction to enumeration

Enumeration is a fancy word for counting – i.e., "how many things are there of a certain type?". Here are some examples of counting problems:

1. How many ways are there to choose 3 odd integers between 0 and 20, if the order matters (i.e., we count the choice $1, 3, 5$ as different from $3, 1, 5$)? (The answer is 1000.)

2. How many ways are there to choose 3 odd integers between 0 and 20, if the order does not matter? (The answer is 220.)

3. How many ways are there to choose 3 distinct odd integers between 0 and 20, if the order matters? (The answer is 720.)

4. How many ways are there to choose 3 distinct odd integers between 0 and 20, if the order does not matter? (The answer is $\dfrac{720}{6} = 120$.)

5. How many prime factorizations does $200 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5$ have (where we count different orderings as distinct)? (The answer is 10.)

6. How many ways are there to tile a 2×15-rectangle with dominos (i.e., rectangles of size 1×2 or 2×1)? (The answer is 987.)

7. How many addends do you get if you expand the product $(a+b)(c+d+e)(f+g)$? (The answer is 12.)

8. How many addends do you get if you expand the product $(a-b)\left(a^2+ab+b^2\right)$? (The answer is 2. In fact, $(a-b)\left(a^2+ab+b^2\right) = a^3 - b^3$.)

9. How many positive divisors does 24 have? (8, namely $1, 2, 3, 4, 6, 8, 12, 24$.)

In this chapter, we will solve a few basic counting problems informally. Then, we will formalize the concepts involved (using the notion of maps = functions = mappings and particularly bijections = bijective maps = one-to-one correspondences), and make rigorous sense of what we have been doing. And then we will finish the remaining counting problems. See Math 222 for much more about counting.

4.1. A refresher on sets

You have seen some set theory, but let me remind you of some concepts and of the notations that I will use.

A set is a collection of objects that knows which objects it contains and which objects it doesn't. That is, if S is a set and p is an object, then S can either contain p (in which case we write $p \in S$) or not contain p (written $p \notin S$). There is no such thing as "containing p twice".

The objects that a set S contains are called the **elements** of S; they are said to **belong** to S, or **lie** in S, or **be contained** in S.

A set can be finite (= contains finitely many objects) or infinite; empty (= contains no objects) or nonempty.

An example of a set is the set of all odd integers. It is infinite. It contains all odd integers and nothing else. Generally, "the set of X" means the set that contains X and nothing else.

Finite sets can be written by listing all their elements. For instance, the set of all odd integers between 0 and 10 can be written as

$$\{1,3,5,7,9\}.$$

The braces { and } around the list are signalling that we mean the set, not the tuple or the single elements themselves. These braces are called "set braces".

Some more examples of finite sets are

$$\begin{aligned}
&\{1,2,3,4,5\},\\
&\{1,2\},\\
&\{1\} \qquad (\text{this is the set that only contains } 1),\\
&\{\} = \varnothing \qquad (\text{this is the empty set}),\\
&\{1,2,\ldots,1000\} \qquad (\text{the meaning of "}\ldots\text{" is clear}).
\end{aligned}$$

Some infinite sets can also be written in this form:

$$\begin{aligned}
&\{1,2,3,\ldots\} \qquad (\text{this is the set of all positive integers});\\
&\{0,1,2,\ldots\} \qquad (\text{this is the set of all nonnegative integers});\\
&\{4,5,6,\ldots\} \qquad (\text{this is the set of all integers } \geq 4);\\
&\{-1,-2,-3,\ldots\} \qquad (\text{this is the set of all negative integers});\\
&\{\ldots,-2,-1,0,1,2,\ldots\} \qquad (\text{this is the set of all integers}).
\end{aligned}$$

Some other sets cannot be written in this form. For instance, how would you list all real numbers? or all rational numbers?

Another way to describe a set is just by putting a description of its elements in set braces. For instance,

$$\begin{aligned}
&\{\text{all integers}\} \qquad (\text{this is the set of all integers});\\
&\{\text{all integers between 3 and 9 inclusive}\};\\
&\{\text{all real numbers}\}.
\end{aligned}$$

Often you want define a set that contains all objects of a certain type that satisfy a certain condition. For example, let's say you want the set of all integers x that satisfy $x^2 < 15$. There is a notation for this:

$$\left\{x \text{ is an integer } \mid\ x^2 < 15\right\}.$$

The vertical bar | here should be read as "such that"; sometimes you use a colon : instead. The part before this bar tells you what type of objects you are

considering to put in the set. The part after this bar is the condition that you impose on these objects. For instance,

$$\begin{aligned}&\Big\{x \text{ is an integer } \mid\ x^2 < 15\Big\}\\ &= \Big\{x \text{ is an integer } :\ x^2 < 15\Big\}\\ &= \{\text{all integers whose square is smaller than } 15\}\\ &= \{-3,-2,-1,0,1,2,3\}\,.\end{aligned}$$

Some sets have standard names:

$$\begin{aligned}\mathbb{Z} &= \{\text{all integers}\} = \{\ldots,-2,-1,0,1,2,\ldots\}\,;\\ \mathbb{N} &= \{\text{all nonnegative integers}\} = \{0,1,2,\ldots\}\\ &\qquad (\text{beware that some authors use } \mathbb{N} \text{ for } \{1,2,3,\ldots\} \text{ instead})\,;\\ \mathbb{Q} &= \{\text{all rational numbers}\}\,;\\ \mathbb{R} &= \{\text{all real numbers}\}\,;\\ \mathbb{C} &= \{\text{all complex numbers}\}\,;\\ \varnothing &= \{\} \qquad (\text{this is the empty set})\,.\end{aligned}$$

Using these notations, we can rewrite

$$\Big\{x \text{ is an integer } \mid\ x^2 < 15\Big\} \qquad \text{as} \qquad \Big\{x \in \mathbb{Z} \mid\ x^2 < 15\Big\}\,.$$

Yet another way of defining sets is when you let a variable range over a given set and collect certain derived quantities. For example,

$$\Big\{x^2+2 \mid\ x \in \{1,3,5,7,9\}\Big\}$$

means the set of all the values x^2+2 for $x \in \{1,3,5,7,9\}$. Thus,

$$\begin{aligned}&\Big\{x^2+2 \mid\ x \in \{1,3,5,7,9\}\Big\}\\ &= \Big\{1^2+2,\ 3^2+2,\ 5^2+2,\ 7^2+2,\ 9^2+2\Big\}\\ &= \{3,\ 11,\ 27,\ 51,\ 83\}\,.\end{aligned}$$

In general, if S is a given set, then the notation

$$\{\text{an expression } \mid\ x \in S\}$$

means the set whose elements are the values of the given expression for all $x \in S$.

Some more examples:

$$\begin{aligned}&\left\{\frac{x+1}{x} \;\middle|\; x \in \{1,2,3,4,5\}\right\}\\ &= \left\{\frac{1+1}{1}, \frac{2+1}{2}, \frac{3+1}{3}, \frac{4+1}{4}, \frac{5+1}{5}\right\}\\ &= \left\{2, \frac{3}{2}, \frac{4}{3}, \frac{5}{4}, \frac{6}{5}\right\}\end{aligned}$$

and

$$\begin{aligned}&\left\{x^2\%5 \;\middle|\; x \in \mathbb{N}\right\}\\ &= \left\{0^2\%5,\ 1^2\%5,\ 2^2\%5,\ 3^2\%5,\ 4^2\%5,\ 5^2\%5,\ \ldots\right\}\\ &= \{0,\ 1,\ 4,\ 4,\ 1,\ 0,\ 1,\ 4,\ 4,\ 1,\ 0,\ 1,\ 4,\ 4,\ 1,\ \ldots\}.\end{aligned}$$

Note that the remainders $x^2\%5$ repeat every five steps, since every integer x satisfies $(x+5)^2 \equiv x^2 \bmod 5$ and therefore $(x+5)^2\,\%5 = x^2\%5$.

Let me repeat that a set cannot contain an element more than once. Also, sets do not come with an ordering of their elements. Thus,

$$\{1,2\} = \{2,1\} = \{2,1,1\} = \{1,2,1,2,1\}.$$

So listing an element twice doesn't force the set to "contain it twice"; it just duplicates the information that the set contains the element.

Thus, the above set $\{0,\ 1,\ 4,\ 4,\ 1,\ 0,\ 1,\ 4,\ 4,\ 1,\ 0,\ 1,\ 4,\ 4,\ 1,\ \ldots\}$ can be rewritten as $\{0,1,4\}$. This is a finite set, even though x ranges through the infinite set $\mathbb{N}$.

Note that sets can contain any mathematical objects, not just numbers. They can contain other sets. Make sure you understand what the sets

$$\{1,2,3\}, \qquad \{\{1,2,3\}\}, \qquad \{\{1,2\},\{3\}\}, \qquad \{\{1\},\{2\},\{3\}\}$$

are and why they are all different.

Sets can be compared and combined in several ways:

Definition 4.1.1. Let A and B be two sets.

(a) We say that A is a **subset** of B (and we write $A \subseteq B$) if every element of A is an element of B.

(b) We say that A is a **superset** of B (and we write $A \supseteq B$) if every element of B is an element of A. This is equivalent to $B \subseteq A$.

(c) We says that $A = B$ if the sets A and B contain the same elements. This is equivalent to saying that both $A \subseteq B$ and $A \supseteq B$ hold.

(d) We define the **union** of A and B to be the set

$$\begin{aligned}A \cup B &:= \{\text{all elements that are contained in } A \text{ or } B\}\\ &= \{x \mid x \in A \text{ or } x \in B\}.\end{aligned}$$

The "or" is non-exclusive, as usual. So $A \cup B$ includes the elements that lie in both A and B as well.

(e) We define the **intersection** of A and B to be the set

$$\begin{aligned} A \cap B &:= \{\text{all elements that are contained in both } A \text{ and } B\} \\ &= \{x \mid x \in A \text{ and } x \in B\}. \end{aligned}$$

(f) We define the **set difference** of A and B to be the set

$$\begin{aligned} A \setminus B &:= \{\text{all elements of } A \text{ that are not contained in } B\} \\ &= \{x \mid x \in A \text{ and } x \notin B\} = \{x \in A \mid x \notin B\}. \end{aligned}$$

Some call this $A - B$.

(g) We say that A and B are **disjoint** if $A \cap B = \varnothing$ (that is, A and B have no element in common).

For example,

$$\begin{aligned} \{1,3,5\} &\subseteq \{1,2,3,4,5\} \qquad \text{but not } \{4,5,6\} \subseteq \{1,2,3,4,5\}; \\ \{1,2,3,4,5\} &\supseteq \{1,3,5\}; \\ \{1,2,3\} &= \{3,2,1\}; \\ \{1,3,5\} \cup \{3,6\} &= \{1,3,5,3,6\} = \{1,3,5,6\}; \\ \{1,3,5\} \cap \{3,6\} &= \{3\}; \\ \{1,2,4\} \cap \{3,5\} &= \varnothing \qquad (\text{that is, } \{1,2,4\} \text{ and } \{3,5\} \text{ are disjoint}); \\ \{3,6\} \setminus \{1,3,5\} &= \{6\}; \\ \mathbb{Z} \setminus \mathbb{N} &= \{-1,-2,-3,\ldots\} = \{\text{all negative integers}\}. \end{aligned}$$

Definition 4.1.2. Several sets $A_1, A_2, \ldots, A_k$ are called **disjoint** if any two of them (not counting a set and itself) are disjoint, i.e., if we have $A_i \cap A_j = \varnothing$ for all $i < j$.

For instance, the three sets $\{1,2\}$, $\{0,7\}$ and $\{5,8,9\}$ are disjoint, but the three sets $\{1,2\}$, $\{0,7\}$ and $\{2,5\}$ are not.

4.2. Counting, informally

Now, let us see how the elements of a set can be counted. Formally speaking, we won't define "counting" until later, so we will be playing around with a vague concept for a while. But you have an intuition for what "counting" means, and it won't mislead you any time soon.

For example, the set of all odd integers between 0 and 10 has 5 elements $(1,3,5,7,9)$, and this doesn't change if you rewrite it as $\{1,3,5,5,5,5,5,7,9\}$.

More generally, I claim:

Proposition 4.2.1. Let $n \in \mathbb{N}$. Then, there are exactly $(n+1)\ //2 = \left\lfloor \dfrac{n+1}{2} \right\rfloor$ odd integers between 0 and n (inclusive).

Proof. The equality $(n+1)\ //2 = \left\lfloor \dfrac{n+1}{2} \right\rfloor$ follows from what we've done a while ago.

It remains to show that there are exactly $\left\lfloor \dfrac{n+1}{2} \right\rfloor$ odd integers between 0 and n. (We will always understand "between" to mean "between (inclusive)".)

We prove this by induction on n:

Base case: For $n = 0$, the claim is true, since there are $0 = \left\lfloor \dfrac{0+1}{2} \right\rfloor$ odd integers between 0 and 0.

Induction step: Let n be a positive integer. Assume (as IH) that the claim holds for $n-1$. That is, assume that there are exactly $\left\lfloor \dfrac{n}{2} \right\rfloor$ odd integers between 0 and $n-1$.

We must prove that the claim also holds for n, meaning that there are exactly $\left\lfloor \dfrac{n+1}{2} \right\rfloor$ odd integers between 0 and n.

The symbol "#" means "number". Thus, our IH says

$$(\#\text{ of odd integers between 0 and } n-1) = \left\lfloor \frac{n}{2} \right\rfloor,$$

and our goal is to prove that

$$(\#\text{ of odd integers between 0 and } n) = \left\lfloor \frac{n+1}{2} \right\rfloor.$$

We are in one of the following two cases:

Case 1: The number n is even.

Case 2: The number n is odd.

First consider Case 1. In this case, n is even. Thus, n is not odd. Hence, the odd integers between 0 and n are precisely the odd integers between 0 and $n-1$. Consequently,

$$\begin{aligned} &(\#\text{ of odd integers between 0 and } n) \\ &= (\#\text{ of odd integers between 0 and } n-1) \\ &= \left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{n+1}{2} \right\rfloor \qquad \left(\begin{array}{c} \text{by the birthday lemma,} \\ \text{since } n+1 \text{ is odd} \end{array} \right). \end{aligned}$$

This proves the claim for n in Case 1.

Now consider Case 2. In this case, n is odd. Hence, the only integer between 0 and n that is not an integer between 0 and $n-1$ is odd. Thus,

$$\begin{aligned}
&(\#\text{ of odd integers between 0 and } n) \\
&= \underbrace{(\#\text{ of odd integers between 0 and } n-1)}_{=\left\lfloor \frac{n}{2} \right\rfloor} + 1 \\
&= \left\lfloor \frac{n}{2} \right\rfloor + 1 = \left\lfloor \frac{n+1}{2} \right\rfloor \qquad \left(\begin{array}{c} \text{by the birthday lemma,} \\ \text{since } n+1 \text{ is even} \end{array} \right).
\end{aligned}$$

This proves the claim for n in Case 2.

So the claim for n is proved in all cases, and the induction step is complete. □

Note: We called the above proof "informal" because we still don't have a rigorous definition of the size of a set (i.e., what "the number of" means). But we will soon see such a definition. Once we know that definition, the above proof will become a formal proof without serious changes.

Here is an even simpler and more basic counting fact: Let's count not the odd integers, but all integers in a given interval.

Proposition 4.2.2. Let $a, b \in \mathbb{Z}$ be such that $a \leq b+1$.

Then, there are exactly $b-a+1$ numbers in the set

$$\{a, a+1, a+2, \ldots, b\} = \{x \in \mathbb{Z} \mid a \leq x \leq b\}.$$

In other words, there are exactly $b-a+1$ integers between a and b (inclusive).

Proof. Induction on b, similar to the above. □

The hard part about this proposition is remembering the "+1"! The set $\{a, a+1, a+2, \ldots, b\}$ is called an integer interval, but unlike intervals in calculus, its size is $b-a+1$, not $b-a$.

Note: If $a, b \in \mathbb{Z}$ are such that $a \leq b-1$, then there are exactly $b-a-1$ integers between a and b (exclusive).

Python's `range(a, b)` is $\{a, a+1, a+2, \ldots, b-1\}$ and contains exactly $b-a$ integers.

Convention 4.2.3. We agree to use the symbol "#" for "number".

4.3. Counting subsets

4.3.1. Counting them all

Let us now count something more interesting than numbers.

How many subsets does the set $\{1,2,3\}$ have? These subsets are

$$\{\}, \quad \{1\}, \quad \{2\}, \quad \{3\},$$
$$\{1,2\}, \quad \{1,3\}, \quad \{2,3\}, \quad \{1,2,3\}.$$

There are 8 of them.

Likewise,

- there are 4 subsets of $\{1,2\}$;
- there are 2 subsets of $\{1\}$,
- there is 1 subset of $\{\}$;
- there are 16 subsets of $\{1,2,3,4\}$.

The pattern is rather hard to miss:

Theorem 4.3.1. Let $n \in \mathbb{N}$. Then,

$$(\#\text{ of subsets of } \{1,2,\ldots,n\}) = 2^n.$$

Informal proof. We induct on n.

Base case: For $n = 0$, the set $\{1,2,\ldots,n\}$ is empty, and thus has only one subset (itself). But 2^0 is also 1.

Induction step: We proceed from $n-1$ to n. Thus, let n be a positive integer. We assume (as IH) that the theorem holds for $n-1$, and try to prove that it holds for n.

So our IH says that

$$(\#\text{ of subsets of } \{1,2,\ldots,n-1\}) = 2^{n-1}.$$

Our goal is to prove that

$$(\#\text{ of subsets of } \{1,2,\ldots,n\}) = 2^n.$$

We define

- a **red set** to be a subset of $\{1,2,\ldots,n\}$ that contains n;
- a **green set** to be a subset of $\{1,2,\ldots,n\}$ that does not contain n.

For example, if $n = 3$, then the red sets are

$$\{3\}, \qquad \{1,3\}, \qquad \{2,3\}, \qquad \{1,2,3\},$$

while the green sets are

$$\{\}, \qquad \{1\}, \qquad \{2\}, \qquad \{1,2\}.$$

Each subset of $\{1,2,\ldots,n\}$ is either red or green, but not both. So

$$(\#\text{ of subsets of } \{1,2,\ldots,n\}) = (\#\text{ of red sets}) + (\#\text{ of green sets}).$$

(This is an instance of the **sum rule** – a basic counting principle saying that we can count objects of two types by adding the numbers of the objects of each type.)

Now let us count the green sets. In fact, the green sets are nothing but the subsets of $\{1,2,\ldots,n-1\}$. Hence,

$$(\#\text{ of green sets}) = (\#\text{ of subsets of } \{1,2,\ldots,n-1\}) = 2^{n-1}$$

by the IH.

Remains to count the red sets. We can reduce this to the # of green sets. Indeed, we can match the red sets up with the green sets as follows: Each green set can be turned into a red set by inserting n into it. Conversely, each red set can be turned into a green set by removing n from it. These two operations are mutually inverse, and so they establish a one-to-one correspondence between the green sets and the red sets. Thus, the # of green sets is the # of red sets. Hence,

$$(\#\text{ of red sets}) = (\#\text{ of green sets}) = 2^{n-1}.$$

Combining what we have shown, we find

$$\begin{aligned}(\#\text{ of subsets of } \{1,2,\ldots,n\}) &= \underbrace{(\#\text{ of red sets})}_{=2^{n-1}} + \underbrace{(\#\text{ of green sets})}_{=2^{n-1}} \\ &= 2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n.\end{aligned}$$

This completes the induction step, and thus the proof of the theorem. □

More generally:

Theorem 4.3.2. Let $n \in \mathbb{N}$. Then, for any n-element set S, we have

$$(\#\text{ of subsets of } S) = 2^n.$$

Informal proof. This follows from the previous theorem, since we can rename the n elements of S as $1,2,\ldots,n$. □

For example,

$$(\#\text{ of subsets of } \{\text{“cat”, “dog”, “rat”}\}) = 2^3.$$

4.3.2. Counting the subsets of a given size

Next, we shall count the subsets of $\{1,2,\ldots,n\}$ that have a given size k. Here, the **size** of a set means the # of its (distinct) elements. For instance, the set $\{1,4,1,7\}$ has size 3, never mind that I needlessly listed the element 1 twice. A set of size k is also known as a **k-element set**. Pretty soon we will give a rigorous definition of size.

For instance, $\{1,2,3,4\}$ is a 4-element set. How many 2-element sets does it have? Six, namely

$$\{1,2\}, \quad \{1,3\}, \quad \{1,4\}, \quad \{2,3\}, \quad \{2,4\}, \quad \{3,4\}.$$

More generally, the answer to the question "how many k-element subsets does a given n-element set have?" turns out to be the binomial coefficient $\binom{n}{k}$. Let us state this as a theorem and give an informal proof (which is easy to turn into a rigorous proof once we have the concepts properly defined):

Theorem 4.3.3. Let $n \in \mathbb{N}$, and let k be any number (not necessarily an integer). Let S be an n-element set. Then,

$$(\#\text{ of } k\text{-element subsets of } S) = \binom{n}{k}.$$

Informal proof. We induct on n (without fixing k). That is, we use induction on n to prove the statement

$$P(n) := \left(\begin{array}{c} \text{"for any number } k \text{ and any } n\text{-element set } S, \\ \text{we have } (\#\text{ of } k\text{-element subsets of } S) = \binom{n}{k}\text{"} \end{array} \right)$$

for each $n \in \mathbb{N}$.

Base case: Let us prove $P(0)$. Let k be any number, and S any 0-element set. Thus, S is the empty set $\varnothing$ (the only 0-element set!). Its only subset is $\varnothing$, which is also a 0-element set. Thus,

$$(\#\text{ of } k\text{-element subsets of } S) = \begin{cases} 1, & \text{if } k = 0; \\ 0, & \text{if } k \neq 0. \end{cases}$$

On the other hand,

$$\binom{n}{k} = \binom{0}{k} = \begin{cases} 1, & \text{if } k = 0; \\ 0, & \text{if } k \neq 0 \end{cases} \qquad \text{(easy to prove)}.$$

Comparing these, we get

$$(\#\text{ of } k\text{-element subsets of } S) = \binom{n}{k}.$$

So $P(0)$ is proved, thus finishing the base case.

Induction step: Let n be a positive integer. Assume (as the IH) that $P(n-1)$ holds. We must prove that $P(n)$ holds.

So we consider any number k and any n-element set S. We must prove that

$$(\#\text{ of } k\text{-element subsets of } S) = \binom{n}{k}.$$

We rename the n elements of S as $1, 2, \ldots, n$, so we must prove that

$$(\#\text{ of } k\text{-element subsets of } \{1, 2, \ldots, n\}) = \binom{n}{k}.$$

To prove this, we define

- a **red set** to be a k-element subset of $\{1, 2, \ldots, n\}$ that contains n;
- a **green set** to be a k-element subset of $\{1, 2, \ldots, n\}$ that does not contain n.

For instance:

- For $n = 4$ and $k = 2$, the red sets are

  $$\{1,4\}, \quad \{2,4\}, \quad \{3,4\},$$

  while the green sets are

  $$\{1,2\}, \quad \{2,3\}, \quad \{1,3\}.$$

- For $n = 5$ and $k = 2$, the red sets are

  $$\{1,5\}, \quad \{2,5\}, \quad \{3,5\}, \quad \{4,5\},$$

  while the green sets are

  $$\{1,2\}, \quad \{1,3\}, \quad \{1,4\}, \quad \{2,3\}, \quad \{2,4\}, \quad \{3,4\}.$$

Each k-element subset of $\{1, 2, \ldots, n\}$ is either red or green (but not both). Hence,

$$\begin{aligned}&(\#\text{ of } k\text{-element subsets of } \{1, 2, \ldots, n\}) \\ &= (\#\text{ of red sets}) + (\#\text{ of green sets}).\end{aligned}$$

The green sets are just the k-element subsets of $\{1, 2, \ldots, n-1\}$. Hence,

$$\begin{aligned}&(\#\text{ of green sets}) \\ &= (\#\text{ of } k\text{-element subsets of } \{1, 2, \ldots, n-1\}) \\ &= \binom{n-1}{k} \qquad \left(\begin{array}{c}\text{by the statement } P(n-1)\text{, which we} \\ \text{have assumed as the IH}\end{array}\right).\end{aligned}$$

Now let's count the red sets.

If T is a red set, then $T \setminus \{n\}$ is a $(k-1)$-element subset of $\{1,2,\ldots,n-1\}$.

Let us refer to the $(k-1)$-element subsets of $\{1,2,\ldots,n-1\}$ as **blue sets**. Thus, if T is a red set, then $T \setminus \{n\}$ is a blue set. Conversely, if Q is a blue set, then $Q \cup \{n\}$ is a red set. This sets up a one-to-one correspondence between the red sets and the blue sets: We turn red sets blue by removing n, and we turn blue sets red by inserting n. Hence,

$$\begin{aligned}
(\#\text{ of red sets}) &= (\#\text{ of blue sets}) \\
&= (\#\text{ of } (k-1)\text{-element subsets of } \{1,2,\ldots,n-1\}) \\
&\qquad\qquad (\text{since this is how we defined blue sets}) \\
&= \binom{n-1}{k-1} \qquad \left(\begin{array}{c}\text{by our IH } P(n-1)\text{, now applied} \\ \text{to } k-1 \text{ instead of } k\end{array}\right).
\end{aligned}$$

Now,

$$\begin{aligned}
&(\#\text{ of } k\text{-element subsets of } \{1,2,\ldots,n\}) \\
&= \underbrace{(\#\text{ of red sets})}_{=\binom{n-1}{k-1}} + \underbrace{(\#\text{ of green sets})}_{=\binom{n-1}{k}} \\
&= \binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k} \qquad (\text{by Pascal's recurrence}).
\end{aligned}$$

This proves $P(n)$, and thus the induction step is complete. □

The above proof can also be used to write an algorithm that lists all the k-element subsets of $\{1,2,\ldots,n\}$. (See the notes.)

The theorem we proved is often called the **combinatorial interpretation of binomial coefficients**, since it reveals that the BCs $\binom{n}{k}$ have a combinatorial meaning at least for $n \in \mathbb{N}$. However, it is just one of many combinatorial interpretations of BCs; we will see a few more in the last chapter.

4.4. Tuples (aka lists)

4.4.1. Definition and disambiguation

Definition 4.4.1. A **finite list** (aka **tuple**) is a lits consisting of finitely many entries (objects of any type). These entries appear in the list in a specified order. They don't have to be distinct.

A finite list is deliminited using parentheses: i.e., the list that contains the entries $a_1, a_2, \ldots, a_n$ in this order is called $(a_1, a_2, \ldots, a_n)$.

"Specified order" means that the list has a well-defined 1st entry, 2nd entry, and so on. Thus, two lists $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_m)$ are considered equal if and only if

- we have $n = m$, and
- we have $a_i = b_i$ for each $i \in \{1, 2, \ldots, n\}$.

For example, $(1,2) \neq (2,1) \neq (2,1,2) \neq (2,2,1)$ (in fact, all these four lists are distinct).

Definition 4.4.2. (a) The **length** of a list $(a_1, a_2, \ldots, a_n)$ is defined to be the number n.
(b) A list of length 2 is called a **pair**.
(c) A list of length 3 is called a **triple**.
(d) A list of length 4 is called a **quadruple**.
(e) A list of length n is called an **n-tuple**.

For example, $(1,3,2,2)$ is a list of length 4 (although it has only 3 distinct entries), i.e., a quadruple of 4-tuple. Likewise, $(5,8)$ is a pair, i.e., a 2-tuple.

There is exactly one list of length 0: the **empty list** $()$.

Lists of length 1 contain just a single entry. For instance: (3).

4.4.2. Counting pairs

- How many pairs (a,b) are there with $a, b \in \{1,2,3\}$? There are nine:

$$\begin{array}{lll} (1,1)\,, & (1,2)\,, & (1,3)\,, \\ (2,1)\,, & (2,2)\,, & (2,3)\,, \\ (3,1)\,, & (3,2)\,, & (3,3)\,. \end{array}$$

  The fact that there are nine is clear from this arrangement: They form a table with 3 rows and 3 columns, where the row determines the first entry of the pair, and the column determines the second entry. Thus, the total number is $3 \cdot 3 = 9$.

- How many pairs (a,b) are there with $a, b \in \{1,2,3\}$ and $a < b$? There are three, namely $(1,2)$ and $(1,3)$ and $(2,3)$.
- How many pairs (a,b) are there with $a, b \in \{1,2,3\}$ and $a = b$? There are three, namely $(1,1)$ and $(2,2)$ and $(3,3)$.
- How many pairs (a,b) are there with $a, b \in \{1,2,3\}$ and $a > b$? There are three, namely $(2,1)$ and $(3,1)$ and $(3,2)$.

Let us generalize this:

Proposition 4.4.3. Let $n \in \mathbb{N}$. Then:
(a) The # of pairs (a,b) with $a,b \in \{1,2,\ldots,n\}$ is n^2.
(b) The # of pairs (a,b) with $a,b \in \{1,2,\ldots,n\}$ and $a < b$ is $1+2+\cdots+(n-1)$.
(c) The # of pairs (a,b) with $a,b \in \{1,2,\ldots,n\}$ and $a = b$ is n.
(d) The # of pairs (a,b) with $a,b \in \{1,2,\ldots,n\}$ and $a > b$ is $1+2+\cdots+(n-1)$.

Informal proof. **(a)** These pairs can be arranged in a table with n rows and n columns, where the rows determine the first entry and the columns determine the second. This table looks as follows:

$$\begin{array}{cccc} (1,1), & (1,2), & \ldots, & (1,n), \\ (2,1), & (2,2), & \ldots, & (2,n), \\ \vdots & \vdots & \ddots & \vdots \\ (n,1), & (n,2), & \ldots, & (n,n). \end{array}$$

So there are $n \cdot n = n^2$ of these pairs.

(b) In the table we have just drawn, a pair (a,b) satisfies $a < b$ if and only if it is placed above the main diagonal. Thus, the # of such pairs is the # of cells above the main diagonal. But this # is

$$0+1+2+\cdots+(n-1),$$

since there are 0 such cells in the last row, 1 such cell in the second-to-last row, 2 such cells in the third-to-last row and so on until the $n-1$ such cells in the top row. So

$$\begin{aligned} &(\text{\# of pairs } (a,b) \text{ with } a,b \in \{1,2,\ldots,n\} \text{ and } a < b) \\ &= 0+1+2+\cdots+(n-1) \\ &= 1+2+\cdots+(n-1). \end{aligned}$$

(c) A pair (a,b) with $a = b$ is just a pair of the form (a,a), that is, a single element of $\{1,2,\ldots,n\}$ written twice in succession. Counting such pairs is therefore equivalent to counting the single elements $a \in \{1,2,\ldots,n\}$; but there are clearly n of them.

(d) The pairs (a,b) that satisfy $a > b$ are in one-to-one correspondence with the pairs (a,b) that satisfy $a < b$: Namely, each former pair becomes a latter pair if we swap its two entries, and vice versa. Thus, the # of former pairs equals the # of latter pairs. But the # of latter pairs is $1+2+\cdots+(n-1)$, as we found above. So the # of former pairs is also $1+2+\cdots+(n-1)$. □

The proposition we just proved has a nice consequence: For any $n \in \mathbb{N}$, we have

$$\begin{aligned}
n^2 &= (\#\text{ of all pairs } (a,b) \text{ with } a,b \in \{1,2,\ldots,n\}) \\
&= (\#\text{ of all pairs } (a,b) \text{ with } a,b \in \{1,2,\ldots,n\} \text{ and } a < b) \\
&\qquad + (\#\text{ of all pairs } (a,b) \text{ with } a,b \in \{1,2,\ldots,n\} \text{ and } a = b) \\
&\qquad + (\#\text{ of all pairs } (a,b) \text{ with } a,b \in \{1,2,\ldots,n\} \text{ and } a > b) \\
&\qquad\qquad \left(\begin{array}{c} \text{since each pair } (a,b) \text{ satisfies either } a < b \text{ or } a = b \text{ or } a > b, \\ \text{and these cases do not overlap} \end{array} \right) \\
&= \underbrace{(1+2+\cdots+(n-1))+n}_{=1+2+\cdots+n} + \underbrace{(1+2+\cdots+(n-1))}_{=(1+2+\cdots+n)-n} \\
&= (1+2+\cdots+n)+(1+2+\cdots+n)-n \\
&= 2\cdot(1+2+\cdots+n)-n.
\end{aligned}$$

Solving this for $1+2+\cdots+n$, we obtain

$$1+2+\cdots+n = \frac{n^2+n}{2} = \frac{n\,(n+1)}{2}.$$

This is the Little Gauss formula.

The same reasoning gives the following more general result:

Theorem 4.4.4. Let $n, m \in \mathbb{N}$. Let A be an n-element set. Let B be an m-element set. Then,

$$(\#\text{ of pairs } (a,b) \text{ with } a \in A \text{ and } b \in B) = nm.$$

What about triples?

Theorem 4.4.5. Let $n, m, p \in \mathbb{N}$. Let A be an n-element set. Let B be an m-element set. Let C be a p-element set. Then,

$$(\#\text{ of triples } (a,b,c) \text{ with } a \in A \text{ and } b \in B \text{ and } c \in C) = nmp.$$

Informal proof. Re-encode each triple (a,b,c) as a pair $((a,b),c)$ (a pair whose first entry is itself a pair). This is a pair whose first entry comes from the set of all pairs (a,b) with $a \in A$ and $b \in B$, whereas its second entry comes from C. Let U be the set of all pairs (a,b) with $a \in A$ and $b \in B$. Then, this set U is an nm-element set by the previous theorem.

Now, we have re-encoded each triple (a,b,c) as a pair $((a,b),c)$ with $(a,b) \in U$ and $c \in C$. Thus,

$$\begin{aligned}
&(\#\text{ of triples } (a,b,c) \text{ with } a \in A \text{ and } b \in B \text{ and } c \in C) \\
&= (\#\text{ of pairs } ((a,b),c) \text{ with } (a,b) \in U \text{ and } c \in C) \\
&= (\#\text{ of pairs } (u,c) \text{ with } u \in U \text{ and } c \in C) \\
&= (nm)\,p
\end{aligned}$$

by the previous theorem (since U is an nm-element set while C is a p-element set). Of course, this simplifies to nmp. The theorem is proved. □

4.4.3. Cartesian products

There is a general notion for sets of pairs:

Definition 4.4.6. Let A and B be two sets.

The set of all pairs (a,b) with $a \in A$ and $b \in B$ is denoted by $A \times B$, and is called the **Cartesian product** of A and B.

For example, $\{7,8\} \times \{1,2,3\}$ is the set of all pairs (a,b) with $a \in \{7,8\}$ and $b \in \{1,2,3\}$. Explicitly, this set consists of the six pairs

$$\begin{array}{lll}
(7,1), & (7,2), & (7,3), \\
(8,1), & (8,2), & (8,3).
\end{array}$$

Likewise, the set $\{1,2\} \times \{2,3\}$ consists of the four pairs

$$\begin{array}{ll}
(1,2), & (1,3), \\
(2,2), & (2,3).
\end{array}$$

A similar notation exists for sets of triples, of quadruples or of k-tuples in general:

Definition 4.4.7. Let $A_1, A_2, \ldots, A_k$ be any k sets.

Then, the set of all k-tuples $(a_1, a_2, \ldots, a_k)$ with $a_1 \in A_1$ and $a_2 \in A_2$ and $\cdots$ and $a_k \in A_k$ is denoted by

$$A_1 \times A_2 \times \cdots \times A_k,$$

and is called the **Cartesian product** (or just **product**) of the sets $A_1, A_2, \ldots, A_k$.

The word "Cartesian" is named after René Descartes, who realized that a point in the plane can be specified by its two coordinates, and a point in space can be specified by its three coordinates. Thus, points in the plane are pairs of real numbers – i.e., the plane is $\mathbb{R} \times \mathbb{R}$ – whereas points in space are triples of real numbers – i.e., space is $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$.

Using the Cartesian product, we can restate our above theorems as follows:

Theorem 4.4.8 (product rule for two sets)**.** Let $n, m \in \mathbb{N}$. Let A be an n-element set. Let B be an m-element set. Then, $A \times B$ is an nm-element set.

Theorem 4.4.9 (product rule for three sets)**.** Let $n, m, p \in \mathbb{N}$. Let A be an n-element set. Let B be an m-element set. Let C be a p-element set. Then, $A \times B \times C$ is an nmp-element set.

More generally:

Theorem 4.4.10 (product rule for k sets)**.** Let $A_1, A_2, \ldots, A_k$ be any k sets. If each A_i is an n_i-element set, then $A_1 \times A_2 \times \cdots \times A_k$ is an $n_1 n_2 \cdots n_k$-element set.

In other words, when you count k-tuples with each entry coming from a certain set, the total number is the product of the numbers of options for each entry.

You can prove this by induction on k, just like we did for triples.

4.4.4. Counting strictly increasing tuples (informally)

Let $n \in \mathbb{N}$.

- Recall that the # of pairs (a, b) of elements of $\{1, 2, \ldots, n\}$ satisfying $a < b$ is
$$1 + 2 + \cdots + (n-1) = \frac{(n-1)\,n}{2} = \binom{n}{2}.$$
- What is the # of triples (a, b, c) of elements of $\{1, 2, \ldots, n\}$ satisfying $a < b < c$?
Such a triple (a, b, c) always determines a 3-element subset of $\{1, 2, \ldots, n\}$, namely $\{a, b, c\}$. Conversely, any 3-element subset of $\{1, 2, \ldots, n\}$ becomes a triple (a, b, c) with $a < b < c$ if we list its elements in increasing order. Thus, the triples (a, b, c) of elements of $\{1, 2, \ldots, n\}$ satisfying $a < b < c$ are just the 3-element subsets of $\{1, 2, \ldots, n\}$ in disguise. Hence,
$$\begin{aligned}&(\#\text{ of triples } (a,b,c) \text{ of elements of } \{1,2,\ldots,n\} \text{ satisfying } a<b<c)\\ &= (\#\text{ of 3-element subsets of } \{1,2,\ldots,n\})\\ &= \binom{n}{3} \qquad \text{(by the combinatorial interpretation of BCs)}.\end{aligned}$$
- More generally: For any $k \in \mathbb{N}$, we have
$$\begin{aligned}&(\#\text{ of } k\text{-tuples } (a_1,a_2,\ldots,a_k) \text{ of elements of } \{1,2,\ldots,n\} \text{ satisfying } a_1<a_2<\cdots<a_k)\\ &= \binom{n}{k}\end{aligned}$$
(by a similar argument: these k-tuples are just the k-element subsets in diguise).

For comparison, if we drop the $a_1 < a_2 < \cdots < a_k$ requirement, we have

$$\begin{aligned}
&(\#\text{ of } k\text{-tuples } (a_1, a_2, \ldots, a_k) \text{ of elements of } \{1, 2, \ldots, n\}) \\
&= \underbrace{nn \cdots n}_{k \text{ times}} \qquad \text{(by the product rule)} \\
&= n^k.
\end{aligned}$$

5. Maps (aka functions)

5.1. Functions, informally

One of the main notions in maths is that of a **function**, aka **map**, aka **mapping**, aka **transformation**.

Intuitively, a function is a "black box" that takes inputs and transforms them into outputs. For instance, the "$f(t) = t^2$" function takes a real number t and outputs its square t^2.

You can thus think of a function as a rule for producing an output from an input. This gives the following **provisional** definition of a function:

Definition 5.1.1 (Informal definition of a function)**.** Let X and Y be two sets. A **function** from X to Y is (provisionally) a rule that transforms each element of X into some element of Y.

If this function is called f, then the result of applying it to a given $x \in X$ will be called $f(x)$ (or sometimes fx).

This is not a real definition: After all, what is a "rule"? But it gives the right intuition. Some comments:

- A function has to "work" for each element of X. It cannot decline to operate on some elements! Thus, "take the reciprocal" is not a function from $\mathbb{R}$ to $\mathbb{R}$, since it does not operate on 0. However, "take the reciprocal" is a function from $\mathbb{R} \setminus \{0\}$ to $\mathbb{R}$.
- A function must not be ambiguous. Each input must produce exactly one output. Thus, "take your number to some random power" is not a function from $\mathbb{R}$ to $\mathbb{R}$.
- We write "$f : X \to Y$" for "f is a function from X to Y".
- Instead of saying "$f(x) = y$", we can say "f transforms x into y" or "f sends x to y" or "f maps x to y" or "f takes the value y at x" or "y is the value of f at x" or "y is the image of x under f" or "applying f to x yields y" or "f takes x to y" or "$f : x \mapsto y$".

For instance, if f is "take the square" from $\mathbb{R}$ to $\mathbb{R}$, then $f(2) = 2^2 = 4$, so that f transforms 2 into 4, or sends 2 to 4, or takes the value 4 at 2, or $f : 2 \mapsto 4$, and so on.

The arrow $\mapsto$ with a bar is for elements; the arrow $\to$ without a bar is for sets. They are not the same.

- The **value** of a function f at an input x means the corresponding output $f(x)$.
- The notation

$$\begin{aligned} &X \to Y, \\ &x \mapsto (\text{some expression involving } x) \end{aligned}$$

(where X and Y are two sets) means "the function from X to Y that sends each element $x \in X$ to the expression to the right of the $\mapsto$ symbol". The expression can be (for instance) x^2 or $\dfrac{1}{x+2}$ or $\dfrac{1}{\sin x + 17}$.

For example,

$$\begin{aligned} &\mathbb{R} \to \mathbb{R}, \\ &x \mapsto x^2 \end{aligned}$$

is the "take the square" function on $\mathbb{R}$ (sending each $x \in \mathbb{R}$ to x^2). For another example,

$$\begin{aligned} &\mathbb{R} \to \mathbb{R}, \\ &x \mapsto \frac{x}{\sin x + 15} \end{aligned}$$

is the function that sends each real number x to $\dfrac{x}{\sin x + 15}$.

For yet another example,

$$\begin{aligned} &\mathbb{R} \to \mathbb{R}, \\ &x \mapsto 2 \end{aligned}$$

is the function that sends each real number x to 2. It is a constant function.

For another example, a function

$$\begin{aligned} &\mathbb{Z} \to \mathbb{Z}, \\ &x \mapsto 2^x \end{aligned}$$

does not exist, since 2^x is not always $\in \mathbb{Z}$. But the function

$$\begin{aligned} &\mathbb{Z} \to \mathbb{Q}, \\ &x \mapsto 2^x \end{aligned}$$

does exist. This function sends each integer x to 2^x.

A more complicated example is the function

$$\begin{aligned} &\mathbb{Z} \to \mathbb{Q}, \\ &x \mapsto \begin{cases} \dfrac{1}{x-1}, & \text{if } x \neq 1; \\ 5, & \text{if } x = 1. \end{cases} \end{aligned}$$

- The notation

$$\begin{aligned} f : X &\to Y, \\ x &\mapsto (\text{some expression involving } x) \end{aligned}$$

means that we take the function from X to Y that sends each $x \in X$ to the expression to the right of the "$\mapsto$" symbol, and we call this function f.

For example, if we write

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto x^2 + 1, \end{aligned}$$

then f henceforth will denote the function from $\mathbb{R}$ to $\mathbb{R}$ that sends each $x \in \mathbb{R}$ to $x^2 + 1$.

- If the set X is finite, then a function $f : X \to Y$ can be specified simply by listing all its values. For instance, we can define a function $f : \{1, 2, 3\} \to \mathbb{Z}$ by setting

$$\begin{aligned} f(1) &= 50; \\ f(2) &= -33; \\ f(3) &= 50. \end{aligned}$$

- If f is a function from X to Y, then the sets X and Y are part of the function. Thus, for example,

$$\begin{aligned} g_1 : \mathbb{Z} &\to \mathbb{Q}, \\ x &\mapsto 2^x \end{aligned}$$

and

$$\begin{aligned} g_2 : \mathbb{N} &\to \mathbb{Q}, \\ x &\mapsto 2^x \end{aligned}$$

and

$$\begin{aligned} g_3 : \mathbb{N} &\to \mathbb{Z}, \\ x &\mapsto 2^x \end{aligned}$$

are three distinct functions! We distinguish between them, so that we can speak of a "domain" and a "target" of a function. Namely, the **domain** of a function $f : X \to Y$ is defined to be the set X, whereas the **target** of this function is defined to be the set Y.

- When are two functions equal? Two functions $f_1 : X_1 \to Y_1$ and $f_2 : X_2 \to Y_2$ are said to be **equal** if and only if

$$\begin{array}{llll} X_1 = X_2 & \text{and} & Y_1 = Y_2 & \text{and} \\ f_1(x) = f_2(x) & \text{for all } x \in X_1. & & \end{array}$$

  An example of two equal functions is

$$\begin{aligned} f_1 : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto x^2 \end{aligned}$$

  and

$$\begin{aligned} f_2 : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto |x|^2 . \end{aligned}$$

At this point, we should have a good idea of what a function is and what can be done with it. Yet, we don't have a rigorous definition. Not all functions are given by explicit formulas, or even by algorithms or lists of values; thus our definition gets unclear once we go beyond such simple cases. This is why we want a rigorous definition. This is our goal in this chapter.

To rigorously define functions, we will first define **relations** – a more general concept. Functions will then be defined as relations with a certain property.

5.2. Relations

Relations (to be specific: binary relations) are another concept you have already seen:

- The relation $\subseteq$ is a relation between two sets. For instance, $\{2,4\} \subseteq \{1,2,3,4\}$ but not $\{2,5\} \subseteq \{1,2,3,4\}$.
- The order relations $\leq$ and $<$ and $>$ and $\geq$ are relations between two integers. For example, $1 \leq 5$ but $1 \not\leq -1$.
- The containment relation $\in$ is a relation between an object and a set. For instance, $3 \in \{1,2,3,4\}$ but $5 \notin \{1,2,3,4\}$.
- The divisibility relation $\mid$ is a relation between integers.

- The relation "coprime" is a relation between integers.
- For any given integer n, the relation "congruence modulo n" is a relation between two integers. For instance, 2 is congruent to 5 modulo 3, but not congruent to 6 modulo 3.
- Plane geometry gives many more examples: "parallel", "perpendicular", "congruent", "similar", ...

All these relations have one thing in common: They can be applied to pairs of objects. Doing so yields a statement that is either true or false.

A general relation R relates elements of a set X with elements of a set Y. For any pair $(x, y) \in X \times Y$ (that is, for any pair consisting of an $x \in X$ and a $y \in Y$), we can apply the relation R to this pair (x, y), obtaining a statement "$x \ R \ y$" which is either true or false. To describe the relation R, we need to know which pairs $(x, y) \in X \times Y$ do satisfy $x \ R \ y$ and which pairs don't. In other words, we need to know the **set** of all pairs $(x, y) \in X \times Y$ that satisfy $x \ R \ y$.

For a rigorous definition, we simply take the relation R to **be** this set of pairs. In other words, we define relations as follows:

Definition 5.2.1. Let X and Y be two sets. A **relation** from X to Y is a subset of $X \times Y$ (that is, a set of pairs (x, y) with $x \in X$ and $y \in Y$).

If R is a relation from X to Y, and if $(x, y) \in X \times Y$ is any pair, then

- we write $x \ R \ y$ if $(x, y) \in R$;
- we write $x \not R \ y$ if $(x, y) \notin R$.

All the relations we have seen so far can be recast in terms of this definition:

- The divisibility relation $|$ is a subset of $\mathbb{Z} \times \mathbb{Z}$, namely the subset

$$\begin{aligned} &\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \text{ divides } y\} \\ &= \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid \text{there exists } z \in \mathbb{Z} \text{ such that } y = xz\} \\ &= \{(x, xz) \mid x, z \in \mathbb{Z}\}. \end{aligned}$$

  For instance, the pairs $(1, 2)$ and $(2, 8)$ and $(4, 12)$ belong to this set, whereas the pairs $(2, 5)$ and $(10, 5)$ and $(8, 2)$ do not.

- The coprimality relation is a subset of $\mathbb{Z} \times \mathbb{Z}$, namely the subset

$$\begin{aligned} &\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \text{ is coprime to } y\} \\ &= \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid \gcd(x, y) = 1\}. \end{aligned}$$

  For instance, it contains the pair $(2, 3)$ and the pair $(7, 9)$, but not $(4, 6)$.

- For any $n \in \mathbb{Z}$, the "congruent modulo n" relation is a subset of $\mathbb{Z} \times \mathbb{Z}$, namely

$$\begin{aligned} &\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \equiv y \bmod n\} \\ &= \{(x,\ x+nz) \mid x,z \in \mathbb{Z}\}. \end{aligned}$$

- If A is any set, then the **equality relation** on A is the subset E_A of $A \times A$ given by

$$\begin{aligned} E_A &= \{(x,y) \in A \times A \mid x = y\} \\ &= \{(x,x) \mid x \in A\}. \end{aligned}$$

  Two elements $x, y \in A$ satisfy $x \ E_A \ y$ if and only if $x = y$.

- We can take literally any subset of $X \times Y$ (where X and Y are two sets), and it will be a relation from X to Y.

A good way to visualize a relation R from a set X to a set Y is by drawing the sets X and Y as blobs, drawing their elements as nodes within these blobs, and drawing an arrow from the x-node to the y-node for every pair (x,y) that belongs to R.

5.3. Functions, formally

We can now rigorously define functions:

Definition 5.3.1 (Rigorous definition of a function)**.** Let X and Y be two sets. A **function** from X to Y means a relation R from X to Y with the following property:

- **Output uniqueness:** For each $x \in X$, there is **exactly one** $y \in Y$ such that $x \ R \ y$.

If R is a function from X to Y, and if x is an element of X, then the unique element $y \in Y$ satisfying $x \ R \ y$ will be called $R(x)$.

In terms of the blobs-and-arrows picture, the "output uniqueness" requirement is saying that each x-node has exactly one arrow outgoing from it. (We don't require anything like this for y-nodes.)

The rigorous definition of a function we just gave is a clarification of the informal definition. In fact, if R is a function from X to Y in the sense of the rigorous definition, then R can be viewed as a rule that sends each input $x \in X$ to the unique $y \in Y$ satisfying $x \ R \ y$; thus R becomes a function in the

informal sense as well. Conversely, if f is a function in the informal sense, then f becomes a function in the rigorous sense as well, namely the relation

$$\{(x,\ f(x))\ \mid\ x \in X\}$$

from X to Y.

From now on, we will consider rigorous and informal functions as the same thing.

5.4. Some more examples of functions

Example 5.4.1. Consider the function

$$f_0 : \{1,2,3,4\} \to \{1,2,3,4\}$$

that sends $1,2,3,4$ to $3,2,3,3$, respectively. As a rigorous function, it is the relation R that satisfies

$$1\ R\ 3, \qquad 2\ R\ 2, \qquad 3\ R\ 3, \qquad 4\ R\ 3$$

and nothing else. In other words, it is the relation

$$\{(1,3),\ (2,2),\ (3,3),\ (4,3)\}.$$

This is just saying that its values are given by the table

$$\begin{array}{cccccc} x & 1 & 2 & 3 & 4 \\ f_0(x) & 3 & 2 & 3 & 3 \end{array}.$$

Example 5.4.2. What about the function

$$\begin{aligned} f_1 : \{1,2,3,4\} &\to \{1,2,3\}, \\ n &\mapsto n\ \ ? \end{aligned}$$

There is no such function, since it would have to send 4 to 4, but $4 \notin \{1,2,3\}$.

Example 5.4.3. Consider the function

$$\begin{aligned} f_2 : \{1,2,3,\ldots\} &\to \{1,2,3,\ldots\}, \\ n &\mapsto (\#\text{ of positive divisors of } n). \end{aligned}$$

As a relation, it is

$$\{(1,1),\ (2,2),\ (3,2),\ (4,3),\ (5,2),\ (6,4),\ (7,2),\ (8,4),\ (9,3),\ \ldots\}$$

(but it is infinite, so we cannot list it completely).

Example 5.4.4. What about the function

$$\begin{aligned}\widetilde{f_2} : \mathbb{Z} &\to \{1,2,3,\ldots\}, \\ n &\mapsto (\#\text{ of positive divisors of } n) \quad ?\end{aligned}$$

There is no such function $\widetilde{f_2}$, since $\widetilde{f_2}(0)$ would have to be undefined or ∞.

Example 5.4.5. What about the function

$$\begin{aligned}f_3 : \{1,2,3,\ldots\} &\to \{1,2,3,\ldots\}, \\ n &\mapsto (\text{the smallest prime divisor of } n) \quad ?\end{aligned}$$

Again, there is no such function f_3, since $f_3(1)$ does not make sense (there is no prime divisor of 1).

But the function f_3 "almosts" exists: Its only undefined value is $f_3(1)$. Removing the offending number 1 from its domain, we obtain the actual function

$$\begin{aligned}\widetilde{f_3} : \{2,3,4,\ldots\} &\to \{1,2,3,\ldots\}, \\ n &\mapsto (\text{the smallest prime divisor of } n).\end{aligned}$$

Example 5.4.6. What about the function

$$\begin{aligned}f_4 : \mathbb{Q} &\to \mathbb{Z}, \\ \frac{a}{b} &\mapsto a \qquad (\text{for all } a, b \in \mathbb{Z} \text{ with } b \neq 0) \quad ?\end{aligned}$$

Restated in a words, this is to be a function that takes a rational number as input, writes it as a ratio of two integers, and outputs the numerator. Is there such a function?

No. This is again a failure of output uniqueness, but this time the problem is not that the output does not exist, but rather that there are too many. For example, if f_4 was a function, then

$$\begin{aligned}f_4(0.5) = f_4\left(\frac{1}{2}\right) &= 1 \qquad \text{would contradict} \\ f_4(0.5) = f_4\left(\frac{2}{4}\right) &= 2.\end{aligned}$$

The underlying issue is that a rational number can be written as a fraction in many different ways, and they have different numerators.

5.5. Well-definedness

The issues we have seen in the last few examples (a supposed function failing to exist because its output values make no sense, or don't lie in the target, or are not unique) are known as **well-definedness** issues. Often, we say that "a function is well-defined" when we mean that it really exists, i.e., its definition does not suffer from such issues.

For example,

- the function

$$\begin{aligned} f_4 : \mathbb{Q} &\to \mathbb{Z}, \\ \frac{a}{b} &\mapsto a \qquad \text{(for all } a, b \in \mathbb{Z} \text{ with } b \neq 0) \end{aligned}$$

  is not well-defined because a is not uniquely determined by $\frac{a}{b}$; but

- the function

$$\begin{aligned} f_5 : \mathbb{Q} &\to \mathbb{Z}, \\ \frac{a}{b} &\mapsto \frac{a^2}{b^2} \qquad \text{(for all } a, b \in \mathbb{Z} \text{ with } b \neq 0) \end{aligned}$$

  is well-defined because $\frac{a^2}{b^2}$ is uniquely determined by $\frac{a}{b}$;

- the function

$$\begin{aligned} f_1 : \{1,2,3,4\} &\to \{1,2,3\}, \\ n &\mapsto n \end{aligned}$$

  is not well-defined because $f_1(4) = 4$ does not lie in the target $\{1,2,3\}$;

- the function

$$\begin{aligned} f_6 : \{1,2,3,4\} &\to \{1,2,3\}, \\ n &\mapsto 1 + (n\%3) \end{aligned}$$

  is well-defined because its outputs at $1,2,3,4$ are $2,3,1,2$.

Thus, to make sure that a function defined by a rule is well-defined (i.e., exists), you have to check that

- its supposed outputs exist (e.g., no division by zero);
- its supposed outputs lie in the target (e.g., no 4 when the target is $\{1,2,3\}$);
- its supposed outputs are determined uniquely by the respective inputs (i.e., no "pick a random power" or "take the numerator").

5.6. The identity function

Definition 5.6.1. For any set A, there is an **identity function** $\mathrm{id}_A : A \to A$. This is the function that sends each $a \in A$ to a itself.

In other words, it is precisely the equality relation E_A.

5.7. Multivariate functions

When the domain of a function f is a Cartesian product of several sets (i.e., its inputs are tuples), f is called a **multivariate function**. For instance, the function

$$\begin{aligned} \mathrm{add} : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}, \\ (a, b) &\mapsto a + b \end{aligned}$$

is a multivariate function. Its input is a pair of two integers (i.e., it has really two inputs), and its output is their sum. As a relation, it is the subset

$$\{((a, b),\ a + b) \mid a, b \in \mathbb{Z}\}$$

of $(\mathbb{Z} \times \mathbb{Z}) \times \mathbb{Z}$. Other multivariate functions are

$$\begin{aligned} \mathrm{sub} : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}, \\ (a, b) &\mapsto a - b \end{aligned}$$

and

$$\begin{aligned} \mathrm{mul} : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}, \\ (a, b) &\mapsto ab \end{aligned}$$

and

$$\begin{aligned} \mathrm{div} : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) &\to \mathbb{Q}, \\ (a, b) &\mapsto a/b \end{aligned}$$

and

$$\begin{aligned} \mathrm{quo} : \mathbb{Z} \times \{1, 2, 3, \ldots\} &\to \mathbb{Z}, \\ (a, b) &\mapsto a//b \end{aligned}$$

and

$$\begin{aligned} \mathrm{rem} : \mathbb{Z} \times \{1, 2, 3, \ldots\} &\to \mathbb{Z}, \\ (a, b) &\mapsto a\%b \end{aligned}$$

(for the last one, we can actually replace $\mathbb{Z}$ by $\mathbb{N}$ in the target).

When f is a multivariate function, its values $f((a_1, a_2, \ldots, a_k))$ will be abbreviated as $f(a_1, a_2, \ldots, a_k)$.

5.8. Composition of functions

The most important way of transforming functions into functions is **composition**:

Definition 5.8.1. Let X, Y and Z be three sets. Let $f : Y \to Z$ and $g : X \to Y$ be two functions. Then, $f \circ g$ denotes the function

$$\begin{aligned} & X \to Z, \\ & x \mapsto f\left(g\left(x\right)\right). \end{aligned}$$

In other words, $f \circ g$ is the function that first applies g and then applies f. It is called the **composition** of f with g, and I pronounce it "f after g".

In terms of relations, if we view f and g as two relations F and G, then $f \circ g$ is the relation

$$\{(x, z) \mid \text{there exists } y \in Y \text{ such that } x \; G \; y \text{ and } y \; F \; z\}$$

from X to Z.

Is composition commutative? In other words, do we always have $f \circ g = g \circ f$? Nope. Firstly, it can happen that $f \circ g$ is well-defined but $g \circ f$ is not (for instance, this happens if $f : \mathbb{N} \to \mathbb{R}$ and $g : \mathbb{Q} \to \mathbb{N}$). Secondly, it can happen that both $f \circ g$ and $g \circ f$ are defined but have different domains (for instance, this happens if $f : \mathbb{N} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{N}$). Thirdly, even if both $f \circ g$ and $g \circ f$ are defined and have the same domains and targets, they might be different. For instance, let $f : \mathbb{R} \to \mathbb{R}$ be the "take the square" function, and $g : \mathbb{R} \to \mathbb{R}$ be the sine function. Then, $\left(f \circ g\right)\left(x\right) = \left(\sin x\right)^2$ but $\left(g \circ f\right)\left(x\right) = \sin\left(x^2\right)$, which are different (usually).

Some basic properties of composition:

Theorem 5.8.2 (associativity of composition)**.** Let $f : Z \to W$ and $g : Y \to Z$ and $h : X \to Y$ be three functions, where X, Y, Z, W are four sets. Then,

$$\left(f \circ g\right) \circ h = f \circ \left(g \circ h\right).$$

Proof. Both $\left(f \circ g\right) \circ h$ and $f \circ \left(g \circ h\right)$ are functions from X to W. Moreover, for each $x \in X$, we have

$$\left(\left(f \circ g\right) \circ h\right)\left(x\right) = \left(f \circ g\right)\left(h\left(x\right)\right) = f\left(g\left(h\left(x\right)\right)\right)$$

and

$$\left(f \circ \left(g \circ h\right)\right)\left(x\right) = f\left(\underbrace{\left(g \circ h\right)\left(x\right)}_{=g\left(h\left(x\right)\right)}\right) = f\left(g\left(h\left(x\right)\right)\right),$$

so that $\left(\left(f \circ g\right) \circ h\right)\left(x\right) = \left(f \circ \left(g \circ h\right)\right)\left(x\right)$. Thus, $\left(f \circ g\right) \circ h = f \circ \left(g \circ h\right)$. □

This theorem allows us to just write $f \circ g \circ h$ without parentheses.

Theorem 5.8.3. Let $f : X \to Y$ be a function. Then,

$$f \circ \mathrm{id}_X = \mathrm{id}_Y \circ f = f.$$

Proof. Very easy. □

5.9. Jectivities (injectivity, surjectivity, bijectivity)

Definition 5.9.1. Let $f : X \to Y$ be a function. Then:
(a) We say that f is **injective** (aka **one-to-one**, aka **an injection**) if

for each $y \in Y$, there exists **at most one** $x \in X$ such that $f(x) = y$.

In other words: We say that f is **injective** if there are no two distinct elements $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$.
(b) We say that f is **surjective** (aka **onto**, aka a **surjection**) if

for each $y \in Y$, there exists **at least one** $x \in X$ such that $f(x) = y$.

In other words: We say that f is **surjective** if every element of Y is an output value of f.
(c) We say that f is **bijective** (aka a **one-to-one correspondence**, aka a **bijection**) if

for each $y \in Y$, there exists **exactly one** $x \in X$ such that $f(x) = y$.

Thus, f is bijective if and only if f is both injective and surjective.

Some examples:

- The function

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N}, \\ k &\mapsto k^2 \end{aligned}$$

is injective (since no two distinct nonnegative(!) integers x_1, x_2 satisfy $x_1^2 = x_2^2$) but not surjective (since $2 \in \mathbb{N}$ is not the square of any nonnegative integer). Thus, it is not bijective.

- Let $S = \{0, 1, 4, 9, 16, \ldots\}$ be the set of all perfect squares. Then, the function

$$\begin{aligned} g : \mathbb{N} &\to S, \\ k &\mapsto k^2 \end{aligned}$$

  is injective (for the same reason as f), but also surjective (since we have restricted its target to its set of outputs), thus bijective.

  Take note: The function f and g differ only in their choice of target! But one is bijective, while the other is not.

- Let $S = \{0, 1, 4, 9, 16, \ldots\}$ be the set of all perfect squares. Then, the function

$$\begin{aligned} g_{\mathbb{Z}} : \mathbb{Z} &\to S, \\ k &\mapsto k^2 \end{aligned}$$

  is not injective (since $g_{\mathbb{Z}}(1) = g_{\mathbb{Z}}(-1)$). It is still surjective, but this does not make it bijective, since it is not injective.

- The function

$$\begin{aligned} h : \mathbb{N} &\to \mathbb{N}, \\ k &\mapsto k//2 \end{aligned}$$

  is surjective (e.g., because each $y \in \mathbb{N}$ satisfies $y = h(2y)$) but not injective (since $h(0) = h(1)$). So it is not bijective.

  However, we can "split it up" into two bijective functions: namely,

$$\begin{aligned} h_{\text{even}} : \{0, 2, 4, 6, \ldots\} &\to \mathbb{N}, \\ k &\mapsto k//2 \end{aligned}$$

  and

$$\begin{aligned} h_{\text{odd}} : \{1, 3, 5, 7, \ldots\} &\to \mathbb{N}, \\ k &\mapsto k//2 \end{aligned}$$

  are both bijections.

- The function

$$\begin{aligned} \text{add} : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}, \\ (a, b) &\mapsto a + b \end{aligned}$$

  is surjective (since each $y \in \mathbb{Z}$ satisfies $y = \text{add}(y, 0)$) but not injective (e.g. because $\text{add}(1, 1) = \text{add}(2, 0)$).

Remark 5.9.2. Consider a function $f : X \to Y$ given by a table of all its values:

$$\begin{array}{cccccc} a & b & c & d & \cdots \\ f(a) & f(b) & f(c) & f(d) & \cdots \end{array}$$

Then:

(a) The function f is injective if and only if the bottom row of this table has no two equal entries.

(b) The function f is surjective if and only if every element of Y appears in the bottom row.

(c) The function f is bijective if and only if every element of Y appears exactly once in the bottom row.

For example, the function

$$\begin{aligned} f : \{4,6,7\} &\to \{0,1,2\}, \\ k &\mapsto k\%3 \end{aligned}$$

has table of values

$$\begin{array}{ccc} 4 & 6 & 7 \\ 1 & 0 & 1 \end{array} ,$$

so it is neither in-, nor surjective (thus not bijective either).

5.10. Inverses

5.10.1. Definition and examples

Bijective maps have a special power: they can be **inverted**. This is defined as follows:

Definition 5.10.1. Let $f : X \to Y$ be a function. An **inverse** of f means a function $g : Y \to X$ such that

$$f \circ g = \mathrm{id}_Y \qquad \text{and} \qquad g \circ f = \mathrm{id}_X .$$

In other words, an **inverse** of f means a function $g : Y \to X$ such that

$$\begin{array}{lll} f(g(y)) = y & \text{for each } y \in Y, & \text{and} \\ g(f(x)) = x & \text{for each } x \in X. & \end{array}$$

Roughly speaking, this is saying that g both undoes f and is undone by f.

Not every function has an inverse. Some examples:

- Let $f : \{1,2,3\} \to \{6,7,8\}$ be the "add 5" function (meaning that $f(k) = k+5$ for each k). Then, f has an inverse, namely the "subtract 5" function $g : \{6,7,8\} \to \{1,2,3\}$. For example, for each $y \in \{6,7,8\}$, we have

$$f(g(y)) = f(y-5) = (y-5)+5 = y.$$

- Let $f : \{1,2,3\} \to \{6,7,8\}$ be the "subtract from 9" function (meaning that $f(k) = 9-k$ for each k). Then, f has an inverse, namely the "subtract from 9" function $g : \{6,7,8\} \to \{1,2,3\}$. (Despite being given by the same formula, f and g are not the same function, since they have different domains.) To see that f is inverse to g, you just check that

$$f(g(y)) = 9-(9-y) = y \qquad \text{and}$$
$$g(f(x)) = 9-(9-x) = x.$$

- Let $f : \{-1,0,1\} \to \{0,1,2\}$ be the "take the square" function ($f(k) = k^2$). Then, f has no inverse. Indeed, any inverse of f would have to send 1 to 1 (since $f(1) = 1$), but at the same time, it would have to send 1 to -1 (since $f(-1) = 1$). But that would contradict output uniqueness. Moreover, any inverse of f would have to send 2 somewhere, but there is nowhere it could go, since 2 is not a value of f. So we have two reasons why f has no inverse.

- Let $f : \{1,2,3\} \to \{1,2,3,4\}$ be the function that sends $1,2,3$ to $1,2,3$, respectively. This function f (despite looking like an identity function) has no inverse, since 4 would have nowhere to go.

5.10.2. Invertibility is bijectivity by another name

The morals of the last two examples are that if a function $f : X \to Y$ is to have an inverse, it must be injective (so that its inverse is never confused about where to send a $y \in Y$) and be surjective (so that each $y \in Y$ has at least somewhere to go under the inverse of f), thus bijective. This turns out to be sufficient as well: If a map is bijective, then it has an inverse. Let us state this as a theorem:

Theorem 5.10.2. Let $f : X \to Y$ be a map between two sets X and Y. Then, f has an inverse if and only if f is bijective.

Proof. See the notes. □

So invertible maps (= maps having inverses) are the same as bijective maps.

5.10.3. Uniqueness of the inverse

Theorem 5.10.3. Let $f : X \to Y$ be a function. Then, f has at most one inverse.

Thus, if f has an inverse, this inverse is unique, and will be called f^{-1}.

Proof. See the notes. □

5.10.4. Inverses of inverses and compositions

Proposition 5.10.4. Let X be any set. Then, the identity map $\mathrm{id}_X : X \to X$ is bijective, and its inverse is id_X itself.

Proposition 5.10.5. Let $f : X \to Y$ be a map that has an inverse $f^{-1} : Y \to X$. Then, $f^{-1} : Y \to X$ has an inverse, namely f.

Theorem 5.10.6 (Socks-and-shoes formula)**.** Let $g : X \to Y$ and $f : Y \to Z$ be two bijective functions, where X, Y, Z are three sets. Then, the composition $f \circ g : X \to Z$ is bijective as well, and its inverse is

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}.$$

(In general, this is not $f^{-1} \circ g^{-1}$.)

See the notes for more examples and solved exercises.

5.11. Isomorphic sets

As an application of bijectivity, we can define the notion of isomorphic sets:

Definition 5.11.1. Let X and Y be two sets. We say that these two sets X and Y are **isomorphic as sets** (or just **isomorphic**, or **in bijection**, or **in one-to-one correspondence**, or **equinumerous**) if there exists a bijective map from X to Y.

This relation "isomorphic" is symmetric: If X and Y are isomorphic, then Y and X are isomorphic, because a bijective map $f : X \to Y$ has a bijective inverse $f^{-1} : Y \to X$.

Some examples:

- The sets $\{1,2\}$ and $\{1,2,3\}$ are **not** isomorphic. In fact, there is no surjective map $f : \{1,2\} \to \{1,2,3\}$ (since there are "not enough arrows" to hit all three elements of $\{1,2,3\}$), and thus no bijective map $f : \{1,2\} \to \{1,2,3\}$.
- The sets $\{1,2,3\}$ and $\{6,7,8\}$ are isomorphic. In fact, the "add 5" map from $\{1,2,3\}$ to $\{6,7,8\}$ is bijective.

- The sets $\{1,2,3\}$ and $\{5,19,27\}$ are isomorphic. For example, the map $f : \{1,2,3\} \to \{5,19,27\}$ that sends $1,2,3$ to $5,19,27$, respectively, is bijective.
- The sets $\mathbb{N}$ and $E := \{\text{all even nonnegative integers}\} = \{0,2,4,6,\ldots\}$ are isomorphic, since the map
$$\begin{aligned} \mathbb{N} &\to E, \\ n &\mapsto 2n \end{aligned}$$
is a bijection.
- The sets $\mathbb{N}$ and $O := \{\text{all odd nonnegative integers}\} = \{1,3,5,7,\ldots\}$ are isomorphic, since the map
$$\begin{aligned} \mathbb{N} &\to O, \\ n &\mapsto 2n+1 \end{aligned}$$
is a bijection.
- The sets $\mathbb{N}$ and $\mathbb{Z}$ are isomorphic, since there is a bijection from $\mathbb{N}$ to $\mathbb{Z}$, since there is a bijection from $\mathbb{N}$ to $\mathbb{Z}$ that sends
$$\begin{aligned} &0,1,2,3,4,5,6,7,8,\ldots && \text{to} \\ &0,1,-1,2,-2,3,-3,4,-4,\ldots, && \text{respectively.} \end{aligned}$$
Explicitly, this bijection f can be defined by the following formula:
$$f(n) = \begin{cases} -n/2, & \text{if } n \text{ is even;} \\ (n+1)/2, & \text{if } n \text{ is odd} \end{cases} \qquad \text{for all } n \in \mathbb{N}.$$
The inverse of f is given by
$$f^{-1}(n) = \begin{cases} 2n-1, & \text{if } n > 0; \\ -2n, & \text{if } n \leq 0 \end{cases} \qquad \text{for all } n \in \mathbb{Z}.$$
- The sets $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$ are isomorphic, since there is a bijection from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$ that sends
$$0,1,2,3,4,5,6,\ldots \qquad \text{to}$$
$$\underbrace{(0,0)}_{\substack{\text{all pairs whose} \\ \text{entries sum to 0}}}, \underbrace{(1,0),\ (0,1)}_{\substack{\text{all pairs whose entries} \\ \text{sum to 1 (ordered by} \\ \text{decreasing first entry)}}}, \underbrace{(2,0),\ (1,1),\ (0,2)}_{\substack{\text{all pairs whose entries} \\ \text{sum to 2 (ordered by} \\ \text{decreasing first entry)}}}, \underbrace{(3,0),\ (2,1),\ (1,2),\ (0,3)}_{\substack{\text{all pairs whose entries} \\ \text{sum to 3 (ordered by} \\ \text{decreasing first entry)}}}, \ldots.$$
The inverse $f^{-1} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ of this bijection f can actually be described by an explicit formula:
$$f^{-1}(n,m) = \frac{(n+m)(n+m+1)}{2} + m.$$

- The sets $\mathbb{N}$ and $\mathbb{Z} \times \mathbb{Z}$ are isomorphic. To see this, we fix a bijection $g : \mathbb{N} \to \mathbb{Z}$ (we constructed one above) and a bijection $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$. Then, consider the map

$$(g * g) \circ f : \mathbb{N} \to \mathbb{Z} \times \mathbb{Z}.$$

  This map sends each nonnegative integer $n \in \mathbb{N}$ to the pair $(g(i), g(j))$, where $(i, j) = f(n)$. Since g is a bijection, $g * g$ is a bijection (by Homework set #6 Exercise 2). Thus, $(g * g) \circ f$ is a composition of two bijections, thus itself a bijection (by Exercise 5.11.1 **(g)** in the notes).

- The sets $\mathbb{N}$ and $\mathbb{Q}$ are isomorphic. This time, we need to list all the rational numbers in an infinite sequence, each appearing exactly once. We can do this as follows: We already know how to list all pairs of integers, since the sets $\mathbb{N}$ and $\mathbb{Z} \times \mathbb{Z}$ are isomorphic. So take such a list, and replace each pair (i, j) by $\frac{i}{j}$. Then remove all the fake fractions $\frac{i}{j}$ with $j = 0$, and remove all the duplicates (i.e., all the non-reduced fractions and all the fractions with negative denominators). This yields a bijection from $\mathbb{N}$ to $\mathbb{Q}$, since each rational number can be uniquely represented as a reduced fraction.

- The sets $\mathbb{N}$ and $\mathbb{R}$ are **not** isomorphic, i.e., there exists no bijection from $\mathbb{N}$ to $\mathbb{R}$. Intuitively, this is because "there are too many real numbers" (a lot more than there are nonnegative integers). A proper proof can be given using the Cantor diagonal argument; see the books of Newstead or Lehman/Leighton/Meyer (references in the notes).

Sets isomorphic to $\mathbb{N}$ are called **countably infinite**. So the last example is saying that $\mathbb{R}$ is uncountably infinite (infinite but not countably infinite). The previous examples are saying that $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{N} \times \mathbb{N}$ and $\mathbb{Z} \times \mathbb{Z}$ are countably infinite.

6. Enumeration revisited

6.1. Counting, formally

6.1.1. Definition

As you have noticed, isomorphic finite sets have the same number of elements – i.e., the same size. We shall now use this to **define** the size of a set!

First some notations:

Definition 6.1.1. (a) If $n \in \mathbb{N}$, then $[n]$ shall mean the set $\{1, 2, \ldots, n\}$.
For instance, $[3] = \{1, 2, 3\}$ and $[1] = \{1\}$ and $[0] = \varnothing$.
(b) If $a, b \in \mathbb{Z}$, then $[a, b]$ shall mean the set

$$\{a, a+1, a+2, \ldots, b\} = \{x \in \mathbb{Z} \mid a \leq x \leq b\}.$$

If $a > b$, then this is understood to be the empty set.
For instance, $[2, 5] = \{2, 3, 4, 5\}$ and $[2, 2] = \{2\}$ and $[2, 0] = \varnothing$.

Now, we define the size of a finite set:

Definition 6.1.2. Let $n \in \mathbb{N}$. A set S is said to have **size** n if S is isomorphic to the set $[n]$ (that is, if there is a bijection from S to $[n]$).

For example:

- The set $\{\text{cat, dog, rat}\}$ has size 3, since the map

$$\begin{aligned} \{\text{cat, dog, rat}\} &\to [3], \\ \text{cat} &\mapsto 1, \\ \text{dog} &\mapsto 2, \\ \text{rat} &\mapsto 3. \end{aligned}$$

  is a bijection.

- The set $[4, 7] = \{4, 5, 6, 7\}$ has size 4, since the map

$$\begin{aligned} [4, 7] &\to [4], \\ k &\mapsto k - 3 \end{aligned}$$

  is a bijection.

- The set $\mathbb{N}$ is infinite, so there is no bijection from $\mathbb{N}$ to $[n]$ no matter what n is. Thus, $\mathbb{N}$ does not have size n for any $n \in \mathbb{N}$.

Here is another equivalent definition of size:

Definition 6.1.3. We define the notion of a "set of size n" recursively:
(a) A set S is said to have **size** 0 if and only if it is empty.
(b) Let n be a positive integer. A set S is said to have **size** n if and only if there exists an $s \in S$ such that $S \setminus \{s\}$ has size $n - 1$.

In other words, a set has size n (for n positive) if and only if we can remove a single element from it and obtain a set of size $n - 1$.

The following can be proved, but we omit the proof:

Theorem 6.1.4. **(a)** The above two definitions of size are equivalent.
(b) The size of a finite set is determined uniquely – i.e., a set cannot have two different sizes at the same time.

Now we introduce some notations for sizes of sets:

Definition 6.1.5. **(a)** An **n-element set** (for some $n \in \mathbb{N}$) means a set of size n.
(b) A set is said to be **finite** if it has size n for some $n \in \mathbb{N}$.
(c) The size of a finite set S will be called $|S|$. It is also called the **cardinality** of S, or the **number** of elements of S. In particular, the **number** of some things means the size of the set of these things.

Thus, our above examples show that

$$|\{\text{cat, dog, rat}\}| = 3 \qquad \text{and} \qquad |[4,7]| = 4.$$

The number of odd integers between 4 and 10 is the size of the set

$$\{\text{odd integers between 4 and 10}\} = \{5,7,9\},$$

and thus equals 3.

6.1.2. Rules for sizes of finite sets

Theorem 6.1.6 (Bijection principle)**.** Let A and B be two finite sets. Then, $|A| = |B|$ if and only if there exists a bijection from A to B.

Theorem 6.1.7. For each $n \in \mathbb{N}$, we have $|[n]| = n$.

Theorem 6.1.8. Let S be a set. Then:
(a) We have $|S| = 0$ if and only if $S = \varnothing$.
(b) We have $|S| = 1$ if and only if $S = \{s\}$.
(c) We have $|S| = 2$ if and only if $S = \{s,t\}$ two distinct elements s and t.

Theorem 6.1.9. Let S be a finite set. Let t be an object such that $t \notin S$. Then,

$$|S \cup \{t\}| = |S| + 1.$$

Theorem 6.1.10 (Sum rule for two sets)**.** Let A and B be two finite disjoint sets (i.e., $A \cap B = \varnothing$). Then, the union $A \cup B$ is again finite, and has size

$$|A \cup B| = |A| + |B|.$$

Theorem 6.1.11 (Sum rule for k sets)**.** Let $A_1, A_2, \ldots, A_k$ be k disjoint finite sets (i.e., $A_i \cap A_j = \varnothing$ for any $i < j$). Then, the union $A_1 \cup A_2 \cup \cdots \cup A_k$ is again finite, and has size

$$|A_1 \cup A_2 \cup \cdots \cup A_k| = |A_1| + |A_2| + \cdots + |A_k|.$$

Theorem 6.1.12 (Difference rule)**.** Let T be a subset of a finite set S. Then:
(a) The set T is finite, and has size $|T| \leq |S|$.
(b) We have $|S \setminus T| = |S| - |T|$.
(c) If $|T| = |S|$, then $T = S$.

Theorem 6.1.13 (Product rule for two sets)**.** Let A and B be two finite sets. Then, the set

$$A \times B = \{\text{all pairs } (a, b) \text{ with } a \in A \text{ and } b \in B\}$$

is again finite and has size

$$|A \times B| = |A| \cdot |B|.$$

Theorem 6.1.14 (Product rule for k sets)**.** Let $A_1, A_2, \ldots, A_k$ be any k finite sets. Then, the set

$$A_1 \times A_2 \times \cdots \times A_k = \{\text{all } k\text{-tuples } (a_1, a_2, \ldots, a_k) \text{ with } a_i \in A_i \text{ for all } i\}$$

is again finite and has size

$$|A_1 \times A_2 \times \cdots \times A_k| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_k|.$$

All these theorems are foundational and known as basic counting rules/principles. We will not prove them.

6.1.3. $A \cup B$ and $A \cap B$ revisited

As a first application of these rules, let me show a "generalized sum rule for two sets":

Theorem 6.1.15. Let A and B be two finite sets (not necessarily disjoint). Then,

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Proof. Restate this claim as

$$|A \cup B| - |A| = |B| - |A \cap B|.$$

By the difference rule, $|(A \cup B) \setminus A| = |A \cup B| - |A|$ (since $A \subseteq A \cup B$) and $|B \setminus (A \cap B)| = |B| - |A \cap B|$ (since $A \cap B \subseteq B$). Thus, we need to show that

$$|(A \cup B) \setminus A| = |B \setminus (A \cap B)|.$$

But this follows from

$$(A \cup B) \setminus A = B \setminus (A \cap B),$$

which you can see on the Venn diagram (both sides are $B \setminus A$) and rigorously prove by showing that each element of one side is contained in the other. □

The theorem we just proved has an analogue for three sets: If A, B and C are three finite sets, then

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

More generally, you can state such a formula for any k finite sets:

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_k| = {} & \sum (\text{sizes of the sets}) \\ & - \sum (\text{sizes of the pairwise intersections}) \\ & + \sum (\text{sizes of the triplewise intersections}) \\ & \pm \cdots \end{aligned}$$

(the signs alternate based on the parity of how many sets you're intersecting). This is known as "Sylvester's sieve formula" or the "principle of inclusion and exclusion". See any textbook on combinatorics or my Math 222 notes from 2022.

6.2. Redoing some proofs rigorously

Let us look back at some informal proofs we've done two chapters ago, and make them rigorous.

See §6.2 in the notes for details. Here is an outline:

We first reproved

$$(\#\text{ of subsets of } S) = 2^n \qquad \text{for any } n\text{-element set } S.$$

Now, let us reprove

Theorem 6.2.1. Let $n \in \mathbb{N}$, and let k be any number (not necessarily an integer). Let S be an n-element set. Then,

$$(\#\text{ of } k\text{-element subsets of } S) = \binom{n}{k}.$$

Rigorous proof (sketched). We induct on n (without fixing k). That is, we use induction on n to prove the statement

$$P(n) := \left(\begin{array}{c} \text{“for any number } k \text{ and any } n\text{-element set } S, \\ \text{we have } (\#\text{ of } k\text{-element subsets of } S) = \dbinom{n}{k} \text{”} \end{array} \right)$$

for each $n \in \mathbb{N}$.

Base case: Let us prove $P(0)$. Let k be any number, and S any 0-element set. Thus, S is the empty set $\varnothing$ (the only 0-element set!). Its only subset is $\varnothing$, which is also a 0-element set. Thus,

$$(\#\text{ of } k\text{-element subsets of } S) = \begin{cases} 1, & \text{if } k = 0; \\ 0, & \text{if } k \neq 0. \end{cases}$$

On the other hand,

$$\binom{n}{k} = \binom{0}{k} = \begin{cases} 1, & \text{if } k = 0; \\ 0, & \text{if } k \neq 0 \end{cases} \qquad (\text{easy to prove}).$$

Comparing these, we get

$$(\#\text{ of } k\text{-element subsets of } S) = \binom{n}{k}.$$

So $P(0)$ is proved, thus finishing the base case.

Induction step: Let n be a positive integer. Assume (as the IH) that $P(n-1)$ holds. We must prove that $P(n)$ holds.

So we consider any number k and any n-element set S. We must prove that

$$(\#\text{ of } k\text{-element subsets of } S) = \binom{n}{k}.$$

To prove this, we pick any $s \in S$ (this exists since $|S| = n > 0$). We define

- a **red set** to be a k-element subset of S that contains s;
- a **green set** to be a k-element subset of S that does not contain s.

Each k-element subset of S is either red or green (but not both). Hence,

$$\{k\text{-element subsets of } S\} = \{\text{red subsets}\} \cup \{\text{green subsets}\},$$

and the two sets $\{\text{red subsets}\}$ and $\{\text{green subsets}\}$ are disjoint. Hence, the sum rule yields

$$\begin{aligned} |\{k\text{-element subsets of } S\}| &= |\{\text{red subsets}\} \cup \{\text{green subsets}\}| \\ &= |\{\text{red subsets}\}| + |\{\text{green subsets}\}|. \end{aligned}$$

In other words,

$$\begin{aligned}&(\#\text{ of } k\text{-element subsets of } S)\\&= (\#\text{ of red sets}) + (\#\text{ of green sets})\,.\end{aligned}$$

The set $\{s\}$ is a subset of S. Hence, the difference rule yields $|S \setminus \{s\}| = \underbrace{|S|}_{=n} - \underbrace{|\{s\}|}_{=1} = n-1$.

The green sets are just the k-element subsets of $S \setminus \{s\}$. Hence,

$$\begin{aligned}&(\#\text{ of green sets})\\&= (\#\text{ of } k\text{-element subsets of } S \setminus \{s\})\\&= \binom{n-1}{k} \qquad \left(\begin{array}{c}\text{by the statement } P(n-1)\text{, which we}\\ \text{have assumed as the IH}\\ \left(\text{since } S \setminus \{s\} \text{ is an } (n-1)\text{-element set}\right)\end{array}\right).\end{aligned}$$

Now let's count the red sets.

If T is a red set, then $T \setminus \{s\}$ is a $(k-1)$-element subset of $S \setminus \{s\}$.

Let us refer to the $(k-1)$-element subsets of $S \setminus \{s\}$ as **blue sets**. Thus, if T is a red set, then $T \setminus \{s\}$ is a blue set. Conversely, if Q is a blue set, then $Q \cup \{s\}$ is a red set. This sets up a bijection

$$\begin{aligned}\{\text{red sets}\} &\to \{\text{blue sets}\}\,,\\ T &\mapsto T \setminus \{s\}\end{aligned}$$

(with inverse map

$$\begin{aligned}\{\text{blue sets}\} &\to \{\text{red sets}\}\,,\\ Q &\mapsto Q \cup \{s\}\end{aligned}$$

). Hence, the bijection principle yields

$$|\{\text{red sets}\}| = |\{\text{blue sets}\}|\,.$$

In other words,

$$\begin{aligned}(\#\text{ of red sets}) &= (\#\text{ of blue sets})\\&= (\#\text{ of } (k-1)\text{-element subsets of } S \setminus \{s\})\\&\qquad\qquad (\text{since this is how we defined blue sets})\\&= \binom{n-1}{k-1} \qquad \left(\begin{array}{c}\text{by our IH } P(n-1)\text{, now applied}\\ \text{to } k-1 \text{ instead of } k\\ \left(\text{since } S \setminus \{s\} \text{ is an } (n-1)\text{-element set}\right)\end{array}\right).\end{aligned}$$

Now,

$$\begin{aligned}
&(\#\text{ of } k\text{-element subsets of } S) \\
&= \underbrace{(\#\text{ of red sets})}_{=\binom{n-1}{k-1}} + \underbrace{(\#\text{ of green sets})}_{=\binom{n-1}{k}} \\
&= \binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k} \qquad \text{(by Pascal's recurrence)}.
\end{aligned}$$

This proves $P(n)$, and thus the induction step is complete. □

Corollary 6.2.2. Let $n \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Proof. This is not the easiest proof, but perhaps the nicest:

Consider the n-element set $[n] = \{1, 2, \ldots, n\}$. This set has size n, so each subset of $[n]$ has size $\leq n$ (by the difference rule). Thus, we can write the set

$$\{\text{subsets of } [n]\}$$

as a union

$$\begin{aligned}
&\{0\text{-element subsets of } [n]\}, \\
&\{1\text{-element subsets of } [n]\}, \\
&\{2\text{-element subsets of } [n]\}, \\
&\ldots, \\
&\{n\text{-element subsets of } [n]\}.
\end{aligned}$$

Moreover, this union is a union of disjoint sets. Therefore, the sum rule for k sets yields

$$\begin{aligned}
&|\{\text{subsets of } [n]\}| \\
&= |\{0\text{-element subsets of } [n]\}| \\
&\qquad + |\{1\text{-element subsets of } [n]\}| \\
&\qquad + |\{2\text{-element subsets of } [n]\}| \\
&\qquad + \cdots \\
&\qquad + |\{n\text{-element subsets of } [n]\}|.
\end{aligned}$$

In other words,

$$\begin{aligned}&(\#\text{ of subsets of } [n])\\ &= (0\text{-element subsets of } [n])\\ &\qquad + (1\text{-element subsets of } [n])\\ &\qquad + (2\text{-element subsets of } [n])\\ &\qquad + \cdots\\ &\qquad + (n\text{-element subsets of } [n])\,.\end{aligned}$$

But we know all the numbers in this equality. Plugging them in, we get

$$2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k}.$$

□

This was an example of a **proof by double counting** – i.e., counting the same thing in two different ways and concluding that the resulting numbers are equal. Many identities can be proved in this way.

6.2.1. Recounting pairs

See §6.2.4 in the text.

6.3. Where do we stand now?

Recall the introductory counting problems from a couple weeks ago. We can now answer some, but not all, of them:

1. How many ways are there to choose 3 odd integers between 0 and 20, if the order matters (i.e., we count the choice $1, 3, 5$ as different from $3, 1, 5$)? (The answer is 1000.)

   We can solve this now: To choose 3 odd integers between 0 and 20, if the order matters, amounts to choosing a 3-tuple (a, b, c) with $a, b, c \in \{1, 3, 5, \ldots, 19\}$. Since the set $\{1, 3, 5, \ldots, 19\}$ has size 10, we conclude that the # of these 3-tuples is $10 \cdot 10 \cdot 10 = 1000$ (by the product rule).

2. How many ways are there to choose 3 odd integers between 0 and 20, if the order does not matter? (The answer is 220.)

   We cannot solve this yet, at least not if the values 3 and 20 are generalized to k and n.

3. How many ways are there to choose 3 distinct odd integers between 0 and 20, if the order matters? (The answer is 720.)

   We cannot solve this yet, at least not if the values 3 and 20 are generalized to k and n.

4. How many ways are there to choose 3 distinct odd integers between 0 and 20, if the order does not matter? (The answer is $\frac{720}{6} = 120$.)

   We can solve this now: This amounts to counting the 3-element subsets of $\{1, 3, 5, \ldots, 19\}$; but this has been done. The answer is $\binom{10}{3} = 120$.

5. How many prime factorizations does $200 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5$ have (where we count different orderings as distinct)? (The answer is 10.)

   We can easily solve this for 200 (since $\binom{5}{2} = 10$) **but not yet the general form** with 200 replaced by n.

6. How many ways are there to tile a 2×15-rectangle with dominos (i.e., rectangles of size 1×2 or 2×1)? (The answer is 987.)

   We cannot solve this yet.

7. How many addends do you get if you expand the product $(a + b)(c + d + e)(f + g)$? (The answer is 12.)

   We can solve this using the product rule: Each addend consists of exactly one of a and b, exactly one of c, d and e, and exactly one of f and g. Thus, these addends are in one-to-one correspondence with the triples $(x, y, z) \in \{a, b\} \times \{c, d, e\} \times \{f, g\}$. There are $2 \cdot 3 \cdot 2 = 12$ such triples by the product rule.

   Note that this relied on the fact that the addends all end up distinct, so they don't cancel or combine.

8. How many addends do you get if you expand the product $(a - b)(a^2 + ab + b^2)$? (The answer is 2. In fact, $(a - b)(a^2 + ab + b^2) = a^3 - b^3$.)

   This is not a combinatorics problem: The answer is 2 because addends cancel.

9. How many positive divisors does 24 have? (8, namely $1, 2, 3, 4, 6, 8, 12, 24$.)

   We cannot solve this yet, at least not in the general case (24 replaced by n). There is a nice formula, but it is beyond our scope (see references in the text).

6.4. Lacunar subsets

6.4.1. Definition

Another type of objects to count are the so-called **lacunar subsets** (aka **sparse subsets** aka ...). Here is their definition:

Definition 6.4.1. A set S of integers is said to be **lacunar** if it contains no two consecutive integers (i.e., if there is no integer i such that both i and $i+1$ belong to S).

For example, $\{2,4,7\}$ is lacunar, but $\{2,4,5\}$ is not. Note that every 1-element set of integers is lacunar, as is the empty set.

Now we can ask ourselves: For given $n \in \mathbb{N}$,

1. how many lacunar subsets does the set $[n] = \{1,2,\ldots,n\}$ have?
2. how many k-element lacunar subsets does the set $[n] = \{1,2,\ldots,n\}$ have for a given $k \in \mathbb{N}$?
3. what is the largest size of a lacunar subset of $[n]$?

We shall answer these all in this section.

6.4.2. The maximum size of a lacunar subset

Question 3 is the easiest to answer, so we start with it:

Proposition 6.4.2. Let $n \in \mathbb{N}$. Then, the maximum size of a lacunar subset of $[n]$ is $\left\lfloor \dfrac{n+1}{2} \right\rfloor$.

Proof. The set

$$\begin{aligned} &\{\text{all odd numbers in } [n]\} \\ &= \{\text{all odd integers between 0 and } n \text{ inclusive}\} \\ &= \{1,3,5,\ldots\} \cap [n] \end{aligned}$$

is a lacunar subset of $[n]$, and has size $\left\lfloor \dfrac{n+1}{2} \right\rfloor$ (easy; Proposition 4.2.1 in the notes). So the size $\left\lfloor \dfrac{n+1}{2} \right\rfloor$ is attainable.

Remains to show that this size $\left\lfloor \dfrac{n+1}{2} \right\rfloor$ is maximum – i.e., if L is a lacunar subset of $[n]$, then

$$|L| \leq \frac{n+1}{2}.$$

There are many ways to do this. Here is just one: Define a new set

$$L^+ := \{\ell + 1 \mid \ell \in L\}.$$

This set L^+ consists of each element of L, incremented by 1. For instance, if $L = \{2,4,7\}$, then $L^+ = \{3,5,8\}$. Thus, $|L^+| = |L|$. But L and L^+ are disjoint (indeed, if $i \in L^+$, then $i = j+1$ for some $j \in L$, and thus $j+1 \notin L$, so that $i \notin L$). Hence, by the sum rule, $|L \cup L^+| = |L| + |L^+| = |L| + |L| = 2 \cdot |L|$.

But $L \cup L^+$ is a subset of $[n+1]$. Thus, by the difference rule, $|L \cup L^+| \leq |[n+1]| = n+1$. Hence,

$$n+1 \geq \left|L \cup L^+\right| = 2 \cdot |L|.$$

Hence, $|L| \leq \dfrac{n+1}{2}$. Since $|L|$ is an integer, this yields $|L| \leq \left\lfloor \dfrac{n+1}{2} \right\rfloor$, qed. □

6.4.3. Counting all lacunar subsets of $[n]$

Now let us count the lacunar subsets of $[n]$. First, we count them all (counting them by size will come later).

With Python or SageMath or any other programming language, we can easily see that the first few values are

n	0	1	2	3	4	5	6	7	8
# of lacunar subsets of $[n]$	1	2	3	5	8	13	21	34	55

,

which reminds us of the Fibonacci sequence given by

$$f_0 = 0, \qquad f_1 = 1, \qquad f_n = f_{n-1} + f_{n-2}.$$

And indeed:

Theorem 6.4.3. For any integer $n \geq -1$, we have

$$(\#\text{ of lacunar subsets of } [n]) = f_{n+2}.$$

Example 6.4.4. The lacunar subsets of $[4]$ are

$$\varnothing,\ \{1\},\ \{2\},\ \{3\},\ \{4\},\ \{1,3\},\ \{2,4\},\ \{1,4\}.$$

So there are 8 of them, which is indeed $f_{4+2} = f_6 = 8$.

Proof of the theorem. For any integer $n \geq -1$, we set

$$\ell_n := (\text{\# of lacunar subsets of } [n]) .$$

We thus must show that

$$\ell_n = f_{n+2} \qquad \text{for each } n \geq -1.$$

We have $\ell_{-1} = 1$ (since the set $[-1] = \varnothing$ has only one lacunar subset, namely $\varnothing$) and $f_{-1+2} = f_1 = 1$. Thus, our claim $\ell_n = f_{n+2}$ holds for $n = -1$. It also holds for $n = 0$.

Let us next show the following:

Claim 1: We have $\ell_n = \ell_{n-1} + \ell_{n-2}$ for each integer $n \geq 1$.

Proof of Claim 1. Let $n \geq 1$ be an integer. We shall call a subset of $[n]$

- **red** if it contains n, and
- **green** if it does not contain n.

Each subset of $[n]$ is either red or green. Hence,

$$\begin{aligned}\ell_n &= (\text{\# of all lacunar subsets of } [n]) \\ &= (\text{\# of red lacunar subsets of } [n]) + (\text{\# of green lacunar subsets of } [n])\end{aligned}$$

by the sum rule.

The green lacunar subsets of $[n]$ are just the lacunar subsets of $[n-1]$. So their # is ℓ_{n-1}.

How do we count the red lacunar subsets of $[n]$? They contain n, so they don't contain $n-1$ (by lacunarity). Thus, if you remove n from them, you get lacunar subsets of $[n-2]$. Conversely, if you insert n into a lacunar subset of $[n-2]$, then you get a red lacunar subset of $[n]$ (its lacunarity is preserved because the missing $n-1$ creates a buffer space before the n). Thus, there is a bijection

$$\begin{aligned}\{\text{red lacunar subsets of } [n]\} &\to \{\text{lacunar subsets of } [n-2]\} , \\ T &\mapsto T \setminus \{n\}\end{aligned}$$

with inverse

$$\begin{aligned}\{\text{lacunar subsets of } [n-2]\} &\to \{\text{red lacunar subsets of } [n]\} , \\ Q &\mapsto Q \cup \{n\} .\end{aligned}$$

Therefore, the bijection principle yields

$$\begin{aligned}&(\text{\# of red lacunar subsets of } [n]) \\ &= (\text{\# of lacunar subsets of } [n-2]) = \ell_{n-2}.\end{aligned}$$

Altogether now,

$$\ell_n = \underbrace{(\text{\# of red lacunar subsets of } [n])}_{=\ell_{n-2}} + \underbrace{(\text{\# of green lacunar subsets of } [n])}_{=\ell_{n-1}}$$
$$= \ell_{n-2} + \ell_{n-1} = \ell_{n-1} + \ell_{n-2}.$$

This proves Claim 1. □

Claim 1 shows that the two sequences $(\ell_{-1}, \ell_0, \ell_1, \ldots)$ and $(f_1, f_2, f_3, \ldots)$ satisfy the same recursion from their third entry on. Since they also agree in their first two entries ($\ell_{-1} = f_1$ and $\ell_0 = f_2$), this entails that they are just identical. That is,

$$\ell_n = f_{n+2} \qquad \text{for each } n \geq -1.$$

(The way to make this argument rigorous is by strong induction – see the notes.) □

6.4.4. Counting the k-element lacunar subsets of $[n]$

The final question about lacunar subsets: How many are there of a given size?

Theorem 6.4.5. Let $n \in \mathbb{Z}$ and $k \in \mathbb{N}$ be such that $k \leq n+1$. Then,

$$(\text{\# of } k\text{-element lacunar subsets of } [n]) = \binom{n+1-k}{k}.$$

The condition $k \leq n+1$ is needed, because for $k > n+1$ the left hand side is 0 while the right hand side is $\binom{\text{negative}}{k} \neq 0$.

There are several ways to prove this. In particular, you can use a red/green induction as before. (The annoying part is to check that $k \leq n+1$ is still valid whenever you apply the IH – or else that you can get the same result without the IH.)

But there is a nicer proof using the bijection principle, not only verifying the theorem but also explaining why it holds. It proceeds by giving a bijection

$$\text{from } \{k\text{-element lacunar subsets of } [n]\}$$
$$\text{to } \{k\text{-element subsets of } [n+1-k]\}.$$

This second proof rests upon a basic feature of finite sets of integers:

Proposition 6.4.6. Let $k \in \mathbb{N}$. Let S be a k-element set of integers. Then, there exists a unique k-tuple $(s_1, s_2, \ldots, s_k)$ of integers satisfying

$$\{s_1, s_2, \ldots, s_k\} = S \qquad \text{and} \qquad s_1 < s_2 < \cdots < s_k.$$

In other words, there is a unique way to list the elements of S in strictly increasing order.

We shall abbreviate this by writing $S = \{s_1 < s_2 < \cdots < s_k\}$.

Now, our bijection

$$\begin{aligned}&\text{from } \{k\text{-element lacunar subsets of } [n]\}\\ &\text{to } \{k\text{-element subsets of } [n+1-k]\}\end{aligned}$$

sends each

$$\{\ell_1 < \ell_2 < \cdots < \ell_k\} \text{ to } \{\ell_1 - 0 < \ell_2 - 1 < \ell_3 - 2 < \cdots < \ell_k - (k-1)\}.$$

Its inverse is a bijection

$$\begin{aligned}&\text{from } \{k\text{-element subsets of } [n+1-k]\}\\ &\text{to } \{k\text{-element lacunar subsets of } [n]\}\end{aligned}$$

that sends each

$$\{s_1 < s_2 < \cdots < s_k\} \text{ to } \{s_1 + 0 < s_2 + 1 < s_3 + 2 < \cdots < s_k + (k-1)\}.$$

See the notes for details.

6.4.5. A corollary

Recall: A subset of $\mathbb{Z}$ is called **lacunar** if and only if it contains no two consecutive integers. Given an integer $n \geq -1$, we have shown that the set $[n] = \{1, 2, \ldots, n\}$ has

- f_{n+2} lacunar subsets in total, and
- $\dbinom{n+1-k}{k}$ lacunar subsets of size k for each given $k \in \{0, 1, \ldots, n+1\}$.

These results have a nice consequence: We have

$$f_{n+2} = \sum_{k=0}^{n} \binom{n+1-k}{k}$$

by the sum rule for k sets, since each lacunar subset of $[n]$ has size $k \in \{0, 1, \ldots, n\}$.

Substituting $n-1$ for n in this formula, we obtain

$$f_{n+1} = \sum_{k=0}^{n-1} \binom{n-k}{k}.$$

So we have proved this for each $n \geq 0$. That is, we have shown that the Fibonacci numbers appear in Pascal's triangle as "diagonal sums". More importantly, we have seen how solving counting problems can lead us to algebraic identities.

Another application of lacunar subsets is counting domino tilings. See the text (§6.4.6) and the references therein.

6.5. Compositions and weak compositions

I have to skip this section for lack of time. See §6.5 in the text. Just a quick idea of what you're missing: How many ways are there to write 4 as a sum of positive integers, if the order matters?

$$\begin{aligned} 4 &= 1+1+1+1 = 1+2+1 = 2+1+1 = 1+1+2 \\ &= 2+2 = 3+1 = 1+3 = 4. \end{aligned}$$

So there are 8 options. Coincidence?

No:

Theorem 6.5.1. Let n be a positive integer. Then, the # of ways to write n as a sum of positive integers (with the order mattering) is

$$\begin{aligned} &\Big(\#\text{ of tuples } (a_1, a_2, \ldots, a_k) \in \{1,2,3,\ldots\}^k \text{ such that } a_1 + a_2 + \cdots + a_k = n\Big) \\ &= 2^{n-1}. \end{aligned}$$

There is a nice bijective proof in the text.

Moreover, we can ask the same question about ways to write n as a sum of k positive integrs for fixed k. The answer is also nice:

Theorem 6.5.2. Let $n, k \in \mathbb{N}$. Then, the # of ways to write n as a sum of k positive integers (with the order mattering) is

$$\begin{aligned} &\Big(\#\text{ of } k\text{-tuples } (a_1, a_2, \ldots, a_k) \in \{1,2,3,\ldots\}^k \text{ such that } a_1 + a_2 + \cdots + a_k = n\Big) \\ &= \binom{n-1}{n-k}. \end{aligned}$$

Again, this is proved bijectively in the text.

There is also this:

Theorem 6.5.3. Let $n, k \in \mathbb{N}$. Then, the # of ways to write n as a sum of k nonnegative integers (with the order mattering) is

$$\begin{aligned} &\Big(\#\text{ of } k\text{-tuples } (a_1, a_2, \ldots, a_k) \in \mathbb{N}^k \text{ such that } a_1 + a_2 + \cdots + a_k = n\Big) \\ &= \binom{n+k-1}{n}. \end{aligned}$$

6.6. Selections

Now we return to a class of problems that we have posed a while ago but never fully answered: counting the ways to select a bunch of elements from a given set.

To be more specific, these problems all have the following form: Given an n-element set S, how many ways are there to select k elements from S (where n and k are fixed $\in \mathbb{N}$) ?

The words "k elements" here are ambiguous, and we get different problems depending on how we read them:

1. Do we want k arbitrary elements or k distinct elements?
2. Does the order of these k elements matter or not? (E.g., would "$1, 2$" and "$2, 1$" count as different selections?)

These choices leave you with 4 options, thus 4 problems. Let us solve them all.

6.6.1. Unordered selections without repetition (= without replacement)

Let us begin with the case when we want to select k distinct elements, with no regard to the order. This just means choosing a k-element subset of S. And we know how many there are: namely $\binom{n}{k}$.

6.6.2. Ordered selections without repetition (= without replacement)

Now we shall study the case when the order does matter. So we are now looking not for subsets, but for k-tuples. But these k-tuples are k-tuples of **distinct** elements. We call such k-tuples **injective**:

Definition 6.6.1. A k-tuple $(i_1, i_2, \ldots, i_k)$ is said to be **injective** if its k entries $i_1, i_2, \ldots, i_k$ are distinct (i.e., if $i_a \neq i_b$ for all $a \neq b$).

For example, the 3-tuple $(6, 2, 5)$ is injective, but $(6, 2, 6)$ is not.

Note that injective tuples are closely related to injective functions: A function $f : [k] \to S$ is injective if and only if the k-tuple $(f(1), f(2), \ldots, f(k))$ is injective.

Some convenient notation:

Definition 6.6.2. Let S be any set, and let $k \in \mathbb{N}$. Then, S^k shall denote the Cartesian product

$$\underbrace{S \times S \times \cdots \times S}_{k \text{ times}} = \{(a_1, a_2, \ldots, a_k) \mid a_1, a_2, \ldots, a_k \in S\}$$
$$= \{k\text{-tuples whose all entries belong to } S\}.$$

For instance,

$$\{a,b\}^3 = \{(a,a,a),\ (a,a,b),\ (a,b,a),\ (a,b,b),\ \ldots,\ (b,b,b)\}.$$

There are eight 3-tuples in this set. None of them is injective. To get injective tuples in S^k, you need $|S| \geq k$.

Now, we know what we are looking for: A way to select k distinct elements from S while the order matters is just an injective k-tuple in S^k. So we must count these injective k-tuples.

Here is the answer:

Theorem 6.6.3. Let $n, k \in \mathbb{N}$. Let S be an n-element set. Then,

$$\left(\#\text{ of injective } k\text{-tuples in } S^k\right) = n\,(n-1)\,(n-2)\cdots(n-k+1).$$

For example,

$$\left(\#\text{ of injective 3-tuples in } \{1,2,3,4,5\}^3\right) = 5 \cdot 4 \cdot 3 = 60.$$

We can rewrite the $n\,(n-1)\,(n-2)\cdots(n-k+1)$ in the above theorem as $k! \cdot \binom{n}{k}$. Observe that it is 0 when $k > n$, which is exactly what we expect given the above observations.

Now, let's prove the theorem: first informally, then formally.

Informal proof. For example, take $n = 5$ and $k = 3$ and $S = \{a,b,c,d,e\}$. We want to count the injective 3-tuples in S^3. Such a 3-tuple has the form (x,y,z), where x, y, z are three distinct elements of $S = \{a,b,c,d,e\}$. So let us see how such a 3-tuple can be chosen:

1. First, we choose its first entry x. There are 5 options, since S has 5 elements.
2. Then, we choose its second entry y. There are 4 options for it, since y can be any of the elements of S except for x.
3. Finally, we choose its third entry z. There are 3 options for it, since z can be any of the elements of S except for x and y (and x and y are distinct).

Altogether, we have 5 options at the first step, then 4 options at the second, then 3 options at the third. Altogether, we can thus choose our 3-tuple in $5 \cdot 4 \cdot 3$ many different ways, because the numbers of options multiply. Here, we have used a counting rule called "**dependent product rule**", which informally says that if we perform a multi-step construction in which we have

- exactly n_1 options in step 1;

- exactly n_2 options in step 2;
- ...;
- exactly n_k options in step k,

then the entire construction can be performed in $n_1 n_2 \cdots n_k$ many ways. Formalized versions of this rule can be found in a few texts like [Loehr] and [Newstead]. But we go another route: We give a more rigorous proof of the theorem that avoids this "dependent product rule" and instead uses induction on k (although the underlying idea is the same). □

Rigorous proof. Forget that we fixed S and n and k. We must thus prove the statement

$$P(k) := \left(\begin{array}{c} \text{"for all } n \in \mathbb{N} \text{ and all } n\text{-element sets } S, \text{ we have} \\ \left(\#\text{ of injective } k\text{-tuples in } S^k\right) = n(n-1)(n-2)\cdots(n-k+1)\text{"} \end{array} \right)$$

for each $k \in \mathbb{N}$. We shall prove this by induction on k.

Base case: We must prove that $P(0)$ holds. This is very easy (see text for details). Essentially, there is only one 0-tuple in S^0, namely the trivial tuple $()$, and it is injective; but the product $n(n-1)(n-2)\cdots(n-k+1)$ is 1 when $k = 0$ because it is an empty product.

Induction step: Let k be a positive integer. Assume (as the IH) that $P(k-1)$ holds. Our goal is to prove $P(k)$.

We have assumed that $P(k-1)$ holds. In other words, for all $n \in \mathbb{N}$ and all n-element sets S, we have

$$\begin{aligned} \left(\#\text{ of injective } (k-1)\text{-tuples in } S^{k-1}\right) &= n(n-1)(n-2)\cdots(n-(k-1)+1) \\ &= n(n-1)(n-2)\cdots(n-k+2). \end{aligned}$$

Now, let us focus on proving $P(k)$. Thus, we fix an $n \in \mathbb{N}$ and an n-element set S, and we set out to prove that

$$\left(\#\text{ of injective } k\text{-tuples in } S^k\right) \stackrel{?}{=} n(n-1)(n-2)\cdots(n-k+1).$$

Let $s_1, s_2, \ldots, s_n$ be the n elements of S (listed without repetition). Then, any

k-tuple in S^k ends with exactly one of $s_1, s_2, \ldots, s_n$. Hence, by the sum rule,

$$\begin{aligned}
&\left(\#\text{ of injective } k\text{-tuples in } S^k\right) \\
&= \left(\#\text{ of injective } k\text{-tuples in } S^k \text{ that end with } s_1\right) \\
&\qquad + \left(\#\text{ of injective } k\text{-tuples in } S^k \text{ that end with } s_2\right) \\
&\qquad + \cdots \\
&\qquad + \left(\#\text{ of injective } k\text{-tuples in } S^k \text{ that end with } s_n\right) \\
&= \sum_{i=1}^{n} \left(\#\text{ of injective } k\text{-tuples in } S^k \text{ that end with } s_i\right).
\end{aligned}$$

Now, let us compute the addends in this sum.

Let $i \in [n]$. How many injective k-tuples in S^k end with s_i ? Such k-tuples have the form

$$(\ldots, s_i),$$

where the "…" are $k-1$ distinct elements of the $(n-1)$-element set $S \setminus \{s_i\}$. Conversely, any k-tuple of this form is an injective k-tuple in S^k that ends with s_i. So we have found a bijection

$$\begin{aligned}
&\text{from } \left\{\text{injective } k\text{-tuples in } S^k \text{ that end with } s_i\right\} \\
&\text{to } \left\{\text{injective } (k-1)\text{-tuples in } \left(S \setminus \{s_i\}\right)^{k-1}\right\}
\end{aligned}$$

that sends each $(\ldots, s_i)$ to the … (that is, removes the last entry). The bijection principle thus yields

$$\begin{aligned}
&\left(\#\text{ of injective } k\text{-tuples in } S^k \text{ that end with } s_i\right) \\
&= \left(\#\text{ of injective } (k-1)\text{-tuples in } \left(S \setminus \{s_i\}\right)^{k-1}\right) \\
&= (n-1)\left((n-1)-1\right)\left((n-1)-2\right)\cdots\left((n-1)-(k-1)+1\right) \\
&\qquad\qquad \left(\begin{array}{c}\text{by our induction hypothesis } P(k-1), \\ \text{applied to } n-1 \text{ and } S \setminus \{s_i\} \text{ instead of } n \text{ and } S\end{array}\right) \\
&= (n-1)(n-2)(n-3)\cdots(n-k+1).
\end{aligned}$$

So forget that we fixed i. We have shown that

$$\begin{aligned}
&\left(\#\text{ of injective } k\text{-tuples in } S^k \text{ that end with } s_i\right) \\
&= (n-1)(n-2)(n-3)\cdots(n-k+1) \qquad \text{for each } i \in [n].
\end{aligned}$$

Now,

$$\begin{aligned}
&\Big(\#\text{ of injective } k\text{-tuples in } S^k\Big) \\
&= \sum_{i=1}^{n} \underbrace{\Big(\#\text{ of injective } k\text{-tuples in } S^k \text{ that end with } s_i\Big)}_{=(n-1)(n-2)(n-3)\cdots(n-k+1)} \\
&= \sum_{i=1}^{n} (n-1)(n-2)(n-3)\cdots(n-k+1) \\
&= n \cdot (n-1)(n-2)(n-3)\cdots(n-k+1) \\
&= n(n-1)(n-2)\cdots(n-k+1).
\end{aligned}$$

This is what we wanted to prove. So $P(k)$ is proved, and with it the theorem. □

6.6.3. Intermezzo: Listing n elements

The theorem we just proved tells us that if S is an n-element set, then the # of ways to choose k distinct elements from S, where the order matters, is

$$n(n-1)(n-2)\cdots(n-k+1) = k! \cdot \binom{n}{k}.$$

In particular, we can apply this to $k = n$, and conclude that the # of ways to choose n distinct elements from S, where the order matters is,

$$n! \cdot \underbrace{\binom{n}{n}}_{=1} = n!.$$

Of course, when we are choosing n distinct elements from an n-element set, we must be choosing all the n elements of the set; the only actual choice is the order. Thus, we have shown (if somewhat informally) the following result:

Corollary 6.6.4. Let $n \in \mathbb{N}$. Let S be an n-element set. Then, the # of ways to list the n elements of S in some order (i.e., the # of n-tuples that contain each element of S exactly once) is $n!$.

6.6.4. Ordered selections with repetition (= with replacement)

We have so far solved two variants of our "select k from n" counting question. We have two more to go: the ones where the k elements are arbitrary (not necessarily distinct). Again, we can either care or not care about the order.

The variant where we do care is the easiest: In this case, we are just counting all k-tuples in S^k. So the # of ways to select k arbitrary elements from an n-element set S, where the order matters, is

$$\left(\#\text{ of all } k\text{-tuples in } S^k\right) = \left|S^k\right| = \left|\underbrace{S \times S \times \cdots \times S}_{k \text{ times}}\right|$$
$$= \underbrace{|S| \cdot |S| \cdot \cdots \cdot |S|}_{k \text{ times}} = |S|^k = n^k.$$

6.6.5. Unordered selections with repetition (= with replacement)

We are left with only one question: What is the # of ways to choose k arbitrary elements from an n-element set S if we **don't** care about their order?

There are several equivalent ways to rigorously define what this means:

1. We can define the notion of a **multiset**, which is "like a finite set but allowing an element to be contained multiple times". I give a few references in the text. Then, a selection of k arbitrary elements of S with no regard to their order is just a size-k multisubset of S.

2. Alternatively, we can define the notion of an **unordered k-tuple**, which is "a k-tuple up to reordering its entries". Formally, these unordered k-tuples are defined as the equivalence classes of usual (i.e., ordered) k-tuples with respect to a certain equivalence relation (again, see text for references). So a selection of k arbitrary elements of S with no regard to their order is just an unordered k-tuple of elements of S.

3. Finally, if we restrict ourselves to the case when $S = [n]$ (which case is sufficient because otherwise you can rename the elements of S as $1, 2, \ldots, n$), then we can use the following "low-tech" solution: We say that a k-tuple $(i_1, i_2, \ldots, i_k) \in S^k$ is **weakly increasing** (aka **sorted in weakly increasing order**) if it satisfies $i_1 \leq i_2 \leq \cdots \leq i_k$. Now, a selection of k arbitrary elements of $S = [n]$, with no regard to their order, can be defined as a weakly increasing k-tuple in S^k. Here, we are using the weakly increasing order to rule out different reorderings of the same k elements.

These three definitions yield different objects, but these objects are equivalent, i.e., there are bijections going between them all. Thus, when it comes to counting, we can pick whatever object we like.

Theorem 6.6.5. Let $n, k \in \mathbb{N}$. Let S be an n-element set. Then,

$$\begin{aligned}&(\#\text{ of ways to select } k \text{ elements from } S \text{ (with no regard for order)})\\ &= \binom{k+n-1}{k}.\end{aligned}$$

See the text for a proof.