Math 221 Section 6 Winter 2024: lecture diary

Darij Grinberg

draft, March 14, 2024

(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

Discrete mathematics is the mathematics of finite, discrete objects: integers, finite sets, graphs (not in this course), polynomials (not in this course) and various further things. Integer sequences, while technically infinite, are still counted as discrete mathematics because you usually only care about specific entries.

Discrete mathematics stands in contrast to **continuous mathematics**, which studies real numbers, continuous functions, infinite sets etc..

Specifically, what we will see in this course are

- **mathematical induction** and **recursion**;
- **elementary number theory** (divisibility, prime numbers, coprimality);
- basic **enumerative combinatorics** (counting, binomial coefficients – see Math 222 for more);
- basic **combinatorial game theory** (2-player games with no randomness).

See the textbook for some further references.

1. Induction and recursion

1.1. The Tower of Hanoi

Let me start with a puzzle called the **Tower of Hanoi**.

You have 3 pegs (or rods). The first peg has n disks stacked on it. The other two pegs are empty. The n disks have n different sizes, and are stacked in the order of decreasing size (biggest disk on the bottom).

You can make a certain kind of moves ("**Hanoi moves**"): You can take the topmost disk from one peg and move it on top of another peg. However, you are only allowed to do this if this disk is smaller than the other disk currently on the latter peg; in other words, you must never stack a larger disk atop a smaller disk.

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

This game can actually be played online (e.g. at https://codepen.io/eliortabeka/pen/yOrrxG).

Let us analyze the $n = 3$ case. In this case, one strategy for winning the game (i.e., achieving the goal) is as follows:

1. Move the smallest disk from peg 1 onto peg 3.

2. Move the middle disk from peg 1 onto peg 2.

3. Move the smallest disk from peg 3 onto peg 2.

4. Move the largest disk from peg 1 onto peg 3.

5. Move the smallest disk from peg 2 onto peg 1.

6. Move the middle disk from peg 2 onto peg 3.

7. Move the smallest disk from peg 1 onto peg 3.

So we can win in 7 moves for $n = 3$.

What about other values of n ? Here are the questions to consider:

Question 1.1.1. **(a)** Can we always win the game?
(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 (since all the disks – i.e., all 0 of them – are already on peg 3). This is optimal.

- For $n = 1$, we win in 1 move. This is optimal.

- For $n = 2$, we win in 3 moves. This is optimal.
- For $n = 3$, we win in 7 moves, as explained above. But do we need 7 moves, or can we win faster?

What about $n = 4$? Solving our questions by brute force gets harder the bigger n gets. But we can try to analyze our strategy for $n = 3$ and see if we can spot some generalizable patterns.

We spot one pattern: The largest disk moves only once. So our strategy for $n = 3$ can be summarized as follows:

1.–3. Move the two smaller disks from peg 1 onto peg 2 (so that the largest disk becomes liberated).

4. Move the largest disk from peg 1 onto peg 3.

5.–7. Move the two smaller disks from peg 2 onto peg 3.

Moreover, the moves 1–3 in this strategy are essentially a Tower of Hanoi game played only with the two smaller disks, except that the goal is not to move them to peg 3 but to move them to peg 2 (but this is clearly equivalent). The largest disk stays at the bottom of peg 1 all the time and does not prevent any of the moves (since all other disks are smaller than it).

Move 4 moves the newly liberated largest disk from peg 1 to peg 3.

Moves 5–7 are another little Tower of Hanoi game for the two smaller disks, except that we now must move them from peg 2 to peg 3. Again, the largest disk does not interfere with the process.

This clarifies the logic behind our strategy.

Does this help us solve the $n = 4$ case? Yes:

1.–7. Move the three smaller disks from peg 1 onto peg 2. (This is a little Tower of Hanoi game for 3 disks.)

8. Move the largest disk to peg 3.

9.–15. Move the three smaller disks from peg 2 onto peg 3. (This is another little Tower of Hanoi game for 3 disks.)

Thus, we don't just have a strategy for $n = 3$ and one for $n = 4$, but actually a "meta-strategy" that lets us win the game for n disks if we know how to win it for $n - 1$ disks. In a nutshell, it says "first move the $n - 1$ smaller disks onto peg 2; then move the largest disk onto peg 3; then move the $n - 1$ smaller disks onto peg 3". We will call this "meta-strategy" just a strategy.

Let us summarize what we gain from this strategy.

Definition 1.1.2. For any integer $n \geq 0$, let m_n denote the # of moves needed to win the game with n disks. If the game acnnot be won with n disks, then we set $m_n = \infty$.

Thus, both of our questions **(a)** and **(b)** boil down to computing m_n.
Here is a table of small values of m_n found using our strategy:

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

.

Note that these values are easily computed using our strategy, because in order to win the game for a given n, we have to win it for $n-1$, then make one extra move, then win it for $n-1$ again. So we get $m_n = m_{n-1} + 1 + m_{n-1} = 2m_{n-1} + 1$ (for all $n \geq 1$).

Right?

Not so fast! We have defined m_n as the smallest # of moves needed to win the n-disks game. But we have only computed the # of moves needed to win the n-disks game **using our strategy**. Maybe our strategy is not the fastest one, and so the true m_n is smaller than the number we have found? Couldn't we perhaps solve the 3-disk game with 6 moves rather than 7 ?

So what we have really proved is the following:

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 (i.e., the sequence of moves) needed to do 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, S_{23} moves $n-1$ disks from peg 1 onto peg 2 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, S_{12} moves $n-1$ disks from peg 2 onto peg 3 in m_{n-1} moves.

Now, we proceed as follows to win the n-disk game:

A. We apply strategy S_{23} to move the $n-1$ smaller disks from peg 1 onto peg 2. (This is allowed because the largest disk rests at the bottom of peg 1 and does not interfere with the movement of smaller disks.)

B. We move the largest disk from peg 1 onto peg 3. (This is allowed since this disk is free (i.e., there are no disks on top of it) and since peg 3 is empty (because all other disks are on peg 2).)

C. We apply strategy S_{12} to move the $n-1$ smaller disks from peg 2 onto peg 3. (This is allowed since the largest disk rests at the bottom of peg 3 and does not interfere.)

This strategy wins the n-disk game in

$$m_{n-1} + 1 + m_{n-1} = 2m_{n-1} + 1$$

moves. So the n-disk game can be won in $2m_{n-1}+1$ many moves. In other words, $m_n \leq 2m_{n-1}+1$. Qed. □

Now, I claim that the inequality $m_n \leq 2m_{n-1}+1$ is actually an equality – i.e., our strategy is optimal.

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. Again, assume that m_{n-1} is an integer.

We need to show that $m_n = 2m_{n-1}+1$. Since we have already proved that $m_n \leq 2m_{n-1}+1$, it remains to prove that $m_n \geq 2m_{n-1}+1$. In other words, it suffices to show that any winning strategy for n disks has at least $2m_{n-1}+1$ many moves.

So let us consider a winning strategy T for n disks. Somewhere during this strategy, the largest disk must be moved (since it must go from peg 1 to peg 3). Let us refer to these moves (i.e., those that move the largest disk) as **special moves**. So T must have at least one special move. (Maybe more than one.)

Before the first special move can happen, the smallest $n-1$ disks must be moved away from peg 1 (to free the largest disk), and must all be gathered on the same peg (otherwise, the largest disk would be prevented from finding a place). This means that before the first special move can happen, we must have already solved the Tower of Hanoi game for $n-1$ disks (perhaps with a different destination peg). By definition, this requires at least m_{n-1} moves. Hence, before the first special move can happen, we already need to have made at least m_{n-1} moves.

Now, consider what happens **after the last special move**. This last special move necessarily moves the largest disk to peg 3. In order for this move to be possible, all the $n-1$ smallest disks must be on the same peg (which is not peg 3), since otherwise the largest disk would either be prevented from getting moved or prevented from finding place on peg 3. Hence, after the last special move, we still need to move the $n-1$ smallest disks onto peg 3. This is a little of Tower of Hanoi game for these $n-1$ smallest disks. As we know, it requires at least m_{n-1} moves.

So, in total, our strategy T needs to have

1. at least m_{n-1} moves before the first special move,

2. at least one special move,

3. at least m_{n-1} moves after the last special move.

Hence, it needs to have at least $m_{n-1} + 1 + m_{n-1} = 2m_{n-1} + 1$ moves in total. This proves $m_n \geq 2m_{n-1} + 1$. □

This proposition confirms our table

n	0	1	2	3	4	5	6	7	8	9	10
m_n	0	1	3	7	15	31	63	127	255	511	1023

.

The equation $m_n = 2m_{n-1} + 1$ is what is called a **recursive formula** for the numbers m_n. This means a formula that allows you to compute m_n using the previous values $m_0, m_1, \ldots, m_{n-1}$. (In the case of our formula, we only need the direct predecessor m_{n-1}.)

Still, can we perhaps do even better? Can we find an **explicit formula** – i.e., one that gives m_n directly? Based on our above table, we suspect that

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

Can we prove this? Not directly, since our strategy is stated only in terms of the $(n-1)$-disk game.

Our last proposition says that $m_n = 2m_{n-1} + 1$ for each $n \geq 1$. Thus, if $m_{n-1} = 2^{n-1} - 1$, then

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

In other words, if our suspected formula $m_n \overset{?}{=} 2^n - 1$ holds for $n-1$, then it also holds for n. For example, if it holds for $n = 3$, then it holds for $n = 4$. Now we can argue as follows:

- The formula $m_n \overset{?}{=} 2^n - 1$ holds for $n = 0$ (since $m_0 = 0$ and $2^0 - 1 = 0$).

- Hence, the formula $m_n \overset{?}{=} 2^n - 1$ holds for $n = 1$ (because if it holds for 0, then it holds for 1).

- Hence, the formula $m_n \overset{?}{=} 2^n - 1$ holds for $n = 2$ (because if it holds for 1, then it holds for 2).

- Hence, the formula $m_n \overset{?}{=} 2^n - 1$ holds for $n = 3$ (because if it holds for 2, then it holds for 3).

- ......
- Hence, the formula $m_n \overset{?}{=} 2^n - 1$ holds for $n = 2024$ (because if it holds for 2023, then it holds for 2024).
- ......

Common sense dictates that this should be a proof of $m_n \overset{?}{=} 2^n - 1$ for all $n \geq 0$. Rigorously, this is not per-se a proof, because a proof must contain a fixed number of steps. So in order to make this mathematically precise, we need to introduce a **principle** (an axiom) that gives legitimacy to this argument. This is the **Principle of Mathematical Induction**:

Theorem 1.1.5 (Principle of Mathematical Induction)**.** Let $P(n)$ be a mathematical statement defined for each integer $n \geq 0$.

(For example, $P(n)$ can be "$n + 1 > n$" or "n is even" or "n is prime" or "there exists a prime number larger than n". Note that not every statement needs to be true. So $P(n)$ is a statement that depends on n; in logic, such a statement is called a **predicate**.)

Assume the following:

1. The statement $P(0)$ holds (i.e., $P(n)$ holds for $n = 0$).
2. For each integer $n \geq 0$, the implication $P(n) \Longrightarrow P(n+1)$ holds (i.e., if $P(n)$ holds, then $P(n+1)$ holds as well).

Then, the statement $P(n)$ holds for every integer $n \geq 0$.

Let me remind you of the meaning of $\Longrightarrow$:

A	B	$A \Longrightarrow B$
true	true	true
true	false	false
false	true	true
false	false	true

For example, $(0 = 1) \Longrightarrow (16 \text{ is odd})$.

1.2. The Principle of Mathematical Induction

The principle we stated last time (and are now going to use to prove our $m_n = 2^n - 1$ formula) is so important that it is worth repeating. We repeat it generalized to b instead of 0:

Theorem 1.2.1 (Principle of Mathematical Induction)**.** Let b be an integer. Let $P(n)$ be a statement defined for each integer $n \geq b$.
Assume the following:

1. The statement $P(b)$ holds (i.e., $P(n)$ holds for $n = b$).

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 as well).

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

Before we discuss the real significance and meaning of this principle, let me show how to use it to prove our $m_n = 2^n - 1$ conjecture. Let me repeat it as a theorem:

Theorem 1.2.2 (explicit answer to Tower of Hanoi)**.** For each integer $n \geq 0$, we let m_n denote the # of moves needed to win the Tower of Hanoi game with n disks (or ∞ if it 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 $b = 0$), it suffices to 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. Let's try to achieve them.

Goal 1 is easy: The statement $P(0)$ is saying that $m_0 = 2^0 - 1$, which is true because both sides are 0. So $P(0)$ holds.

We now start working towards Goal 2. Let $n \geq 0$ be an integer. We must prove the implication $P(n) \Longrightarrow P(n+1)$. So we assume that $P(n)$ holds, and we set out to prove that $P(n+1)$ holds.

Our assumption says that $P(n)$ holds, i.e., that $m_n = 2^n - 1$. In particular, m_n is an integer, i.e., the Hanoi game for n disks is winnable.

We need to prove that $P(n+1)$ holds, i.e., that $m_{n+1} \overset{?}{=} 2^{n+1} - 1$.

Our last proposition says that $m_n = 2m_{n-1} + 1$ if $n \geq 1$. But this is not very helpful, since we want m_{n+1}, which is not part of this equality.

But we can also apply our last proposition to $n+1$ instead of n (since n was just an arbitrary positive integer in that proposition; it is not bound to be our current n). This gives us

$$m_{n+1} = 2m_n + 1.$$

Thus,

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

But this is precisely the statement $P(n+1)$. So we have shown that $P(n+1)$ holds.

More precisely, we have shown that $P(n+1)$ holds under the assumption that $P(n)$ holds. In other words, we have proved the implication $P(n) \Longrightarrow P(n+1)$. This achieves Goal 2.

Now that we have achieved both goals, the Principle of Mathematical Induction ensures that $P(n)$ holds for each integer $n \geq 0$. In other words, $m_n = 2^n - 1$ holds for each integer $n \geq 0$. This proves the theorem. □

What have we really done here? How did this proof work? What is the logic behind the Principle of Mathematical Induction?

Let us take a look at the structure of the above proof.

Our goal was to show that $P(n)$ holds for each $n \geq 0$.

In other words, our goal was to prove the infinite chain of statements

$$P(0), \quad P(1), \quad P(2), \quad P(3), \quad \ldots$$

We have proved directly that $P(0)$ holds; this was Goal 1.

We have then proved that $P(n) \Longrightarrow P(n+1)$ for each n. In other words, we have proved that each statement in our chain implies the next. In particular, $P(0) \Longrightarrow P(1)$ and $P(1) \Longrightarrow P(2)$ and $P(2) \Longrightarrow P(3)$ and so on.

Combining $P(0)$ with $P(0) \Longrightarrow P(1)$, we get $P(1)$.

Combining $P(1)$ with $P(1) \Longrightarrow P(2)$, we get $P(2)$.

Combining $P(2)$ with $P(2) \Longrightarrow P(3)$, we get $P(3)$.

And so on. Clearly, by continuing this reasoning, you can get to any statement in this chain. So, for each $n \geq 0$, you conclude that $P(n)$ holds by doing n steps of this argument.

Strictly speaking, this does not follow, because a proof can only have a given fixed number of steps. But it is convincing if you have common sense. The Principle of Mathematical Induction formalizes this common-sense argument: It says that if each statement implies the next, and if the first statement $P(0)$ is true, then each statement in the chain is true.

Common metaphors for the Principle of Mathematical Induction:

- You can think of the statements $P(0), P(1), P(2), \ldots$ as infinitely many lamps arranged in a row, daisy-chained so that if you turn on $P(n)$ then $P(n+1)$ also goes on. Thus, turning on $P(0)$ will trigger each lamp eventually.

- You can think of the statements $P(0)$, $P(1)$, $P(2)$, ... as dominos arranged in a row, sufficiently close to one another that tipping over any of them will tip over the next. Thus, after you tip over the first domino $P(0)$, all the other dominos will eventually fall down.

I called the Principle of Mathematical Induction a theorem, but it really is an axiom. Any text that proves it necessarily uses some other axiom that formalizes the same idea.

1.3. Some more proofs by induction

A proof that uses the Principle of Mathematical Induction is called a **proof by induction** (or an **induction proof**, or an **inductive proof**). So our proof of $m_n = 2^n - 1$ was a proof by induction.

Let us see some more such proofs.

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 (= left hand side) of this equation is understood to be the sum of the first n positive integers. For $n = 0$, this sum is an empty sum (i.e., a sum with no addends), 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 $s_n = \frac{n(n+1)}{2}$ for each $n \geq 0$.

Let us denote this statement "$s_n = \frac{n(n+1)}{2}$" by $P(n)$. So we need to prove that $P(n)$ holds for each $n \geq 0$.

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.

For Goal 1, we observe that the statement $P(0)$ just says $s_0 = \dfrac{0(0+1)}{2}$, which is true because both sides are 0 (indeed, $s_0 = 1 + 2 + \cdots + 0$ is an empty sum and thus equals 0 by definition).

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

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

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

We must prove $P(n+1)$. In other words, we must prove that

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

To do so, we observe that

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

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

We have now achieved both goals, so the Principle of Mathematical Induction yields that $P(n)$ holds for each $n \geq 0$. This proves the theorem. □

Supposedly, Little Gauss did not prove the theorem this way; instead he used a trick:

Second proof of the Little Gauss formula. We have

$$\begin{aligned} & 2 \cdot (1 + 2 + \cdots + n) \\ &= (1 + 2 + \cdots + n) + (1 + 2 + \cdots + n) \\ &= (1 + 2 + \cdots + n) + (n + (n-1) + \cdots + 1) \\ &= \underbrace{(1+n)}_{=n+1} + \underbrace{(2 + (n-1))}_{=n+1} + \underbrace{(3 + (n-2))}_{=n+1} + \cdots + \underbrace{(n+1)}_{=n+1} \\ &= \underbrace{(n+1) + (n+1) + (n+1) + \cdots + (n+1)}_{n \text{ times}} = n \cdot (n+1). \end{aligned}$$

Dividing by 2, we obtain

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

qed. □

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

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

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

Proof. This will be an almost-verbatim copy of the first proof of the Little Gauss formula. We just change what we need to change.

We set

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

Thus, we must prove that $s_n = \dfrac{n(n+1)(2n+1)}{6}$ for each $n \geq 0$.

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

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.

For Goal 1, we observe that the statement $P(0)$ just says $s_0 = \dfrac{0(0+1)(2 \cdot 0+1)}{6}$, which is true because both sides are 0 (indeed, $s_0 = 1^2 + 2^2 + \cdots + 0^2$ is an empty sum and thus equals 0 by definition).

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

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

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

To do so, we observe that

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

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

We have now achieved both goals, so the Principle of Mathematical Induction yields that $P(n)$ holds for each $n \geq 0$. This proves the theorem. □

Exercise 1.3.1. Prove that

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^3$$

for each nonnegative integer n.

1.4. Notations for an induction proof

We will be using the Principle of Mathematical Induction a lot. Here is some standard terminology commonly used in proofs that use this principle. Let us 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 does not have to be called n. Your statement might as well be "for every integer $a \geq 0$, we have [...]", in which case you can prove it by inducting on a.

- The proof of $P(b)$ (this was Goal 1 in our above proofs) is called the **induction base** or the **base case**. In our above examples, b was 0, but it can be any integer. For instance, 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 induction base consists in proving that $2^4 \geq 4^2$.

- The proof of the "$P(n) \Longrightarrow P(n+1)$ for every $n \geq b$" claim (that is, Goal 2 in our above proofs) is called the **induction step**. For example, in our last proof, this was the part where we assumed that

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

  and proved that

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

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

As an example, let us rewrite our above proof of the Tower of Hanoi answer ($m_n = 2^n - 1$) using this language:

Proof of the Tower of Hanoi theorem, rewritten. We induct on n.

Base case: For $n = 0$, the theorem holds, since both sides equal 0.

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 must now prove that it holds for $n+1$ as well (this is what we called $P(n+1)$).

We have assumed that the theorem holds for n. In other words, $m_n = 2^n - 1$. This is our induction hypothesis.

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

To prove this, we apply the last proposition to $n+1$ instead of n and obtain

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

Thus, the induction goal is reached, and the induction is complete. The theorem is proved. □

1.5. The Fibonacci numbers

1.5.1. Definition

Our next applications of induction will be some properties of the **Fibonacci sequence**:

> **Definition 1.5.1.** The **Fibonacci sequence** is the sequence $(f_0, f_1, f_2, \ldots)$ of nonnegative integers defined recursively by setting
>
> $$f_0 = 0, \qquad f_1 = 1, \qquad \text{and}$$
> $$f_n = f_{n-1} + f_{n-2} \qquad \text{for each } n \geq 2.$$

In other words, the Fibonacci sequence starts with the two entries 0 and 1, and then each next entry is the sum of the previous two entries. This is a **recursive** definition, meaning that it does not directly define each entry, but rather defines it in terms of the entries before it.

The entries of the Fibonacci 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 lets you compute (for example) f_{13} by first computing $f_0, f_1, \ldots, f_{12}$ in this order.

1.5.2. The sum of the first n positive Fibonacci numbers

The Fibonacci sequence is famous for its many properties; here is maybe the simplest one:

> **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 $n = 8$, this is saying that

$$1 + 1 + 2 + 3 + 5 + 8 + 13 + 21 = 55 - 1.$$

Proof. We induct on n.

Base case: For $n = 0$, the theorem claims that $f_1 + f_2 + \cdots + f_0 = f_{0+2} - 1$, which is true since the LHS (= left hand side) is an empty sum (and thus 0 by definition), whereas the RHS is $f_{0+2} - 1 = f_2 - 1 = 1 - 1 = 0$.

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

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

We must prove that

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

We have

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

This is precisely what we wanted to prove – i.e., the induction goal is achieved. This completes the induction step. Thus, the theorem is proved. □

1.6. Some more examples of induction

Here is another example of a proof by induction, and incidentally a useful formula:

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 equality $2^0 + 2^1 + \cdots + 2^{n-1} = 2^n - 1$ is true, since the LHS is an empty sum and thus equals 0, whereas the RHS is $2^0 - 1 = 0$.

Induction step: Let n be an integer ≥ 0. Assume that the theorem holds for n, i.e., that we have

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

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

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

However,

$$\begin{aligned} 2^0 + 2^1 + \cdots + 2^{(n+1)-1} &= 2^0 + 2^1 + \cdots + 2^n \\ &= \underbrace{\left(2^0 + 2^1 + \cdots + 2^{n-1}\right)}_{\substack{=2^n-1 \\ \text{(by the induction hypothesis)}}} + 2^n \\ &= \left(2^n - 1\right) + 2^n = 2 \cdot 2^n - 1 = 2^{n+1} - 1. \end{aligned}$$

This achieves the induction goal, and thus the induction proof is complete. □

This theorem can be generalized:

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 in the parentheses is the sum of all products x^iy^j where i and j are nonnegative integers with $i + j = n - 1$.

Before we prove this, let us give some examples for what this theorem says:

- For $n = 2$, the theorem says that
$$(x-y)(x+y) = x^2 - y^2.$$
- For $n = 3$, the theorem says that
$$(x-y)\left(x^2 + xy + y^2\right) = x^3 - y^3.$$
- For $n = 4$, the theorem says that
$$(x-y)\left(x^3 + x^2y + xy^2 + y^3\right) = x^4 - y^4.$$
- For $x = 2$ and $y = 1$, the theorem says that
$$(2-1)\left(2^{n-1} + 2^{n-2}1 + 2^{n-3}1^2 + \cdots + 2^21^{n-3} + 2 \cdot 1^{n-2} + 1^{n-1}\right) = 2^n - 1^n.$$
Since any power of 1 is 1, and since $2 - 1 = 1$, this can be simplified to
$$2^{n-1} + 2^{n-2} + 2^{n-3} + \cdots + 2^2 + 2 + 1 = 2^n - 1.$$
This is just another way to write
$$2^0 + 2^1 + \cdots + 2^{n-1} = 2^n - 1.$$
So we are generalizing the preceding 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 RHS is $x^0 - y^0 = 1 - 1 = 0$, whereas the LHS is also 0 since the huge sum is empty.

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

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

We begin by extracting the y^n addend from the long sum. We thus obtain

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

which is exactly what we need to prove. So the induction step is complete, and the theorem proved. □

Corollary 1.6.3. Let q be a number distinct from 1. Let $n \geq 0$ be an integer. Then,

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

Proof. Apply the above theorem to $x = q$ and $y = 1$. This gives

$$(q-1)\left(q^{n-1} + q^{n-2}1 + q^{n-3}1^2 + \cdots + q^2 1^{n-3} + q \cdot 1^{n-2} + 1^{n-1}\right) = q^n - 1^n.$$

Simplifying this, we find

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

Dividing this by $q-1$, we find

$$q^{n-1}+q^{n-2}+q^{n-3}+\cdots+q^2+q+1=\frac{q^n-1}{q-1}.$$

But the LHS here is just the sum $q^0+q^1+q^2+\cdots+q^{n-1}$, written in reverse. So the corollary is proved. □

1.7. How to not use induction

Induction proofs can be slippery:

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

Proof. We induct on n:

Base case: This is clearly true for $n=1$, since a single horse has just one color.

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

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

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

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

Also by the 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}. These two horses have the same color as the "middle horses" $H_2, H_3, \ldots, H_n$ (by the previous two paragraphs). Thus, all $n+1$ horses have the same color. This completes the induction step, and thus the theorem is proved.

But the theorem is clearly false. One way to debug a proof of a false theorem is by looking at an example where the theorem is false, and tracking down the error on this example. The simplest example where the above theorem is false is the case of 2 horses of different color. So there must be an error in the induction step for $n=1$ (since this step takes us from the true fact that any 1 horse has the same color to the false fact that any 2 horses have the same color).

Let us see how the induction step argues for $n=1$. Here the $n+1$ horses $H_1, H_2, \ldots, H_{n+1}$ are just the two horses H_1 and H_2. Our induction step argues that the first horse H_1 and the last horse $H_{n+1}=H_2$ have the same color as the "middle horses" $H_2, H_3, \ldots, H_1$. There are no middle horses! It makes no sense to say that a horse has the same color as a non-existing horse. So the argument breaks down. The underlying logical misconception is not a problem with induction; it is rather the fact that transitivity of equality holds for single objects ($a = b$ and $c = b$ imply $a = c$) but not for empty lists ($a = b_1 = b_2 = \cdots = b_n$ and $c = b_1 = b_2 = \cdots = b_n$ imply $a = c$ only when $n > 0$). □

Note how one litte mistake has brought down the entire proof! For an induction proof to work, the induction step needs to work for all n; that is, we need the implication $P(n) \Longrightarrow P(n+1)$ to hold for each n. If even one of these implications breaks down, the whole chain gets disconnected, and all the statements $P(n)$ after this point are no longer guaranteed to hold. For example, if we have a statement $P(n)$ for each $n \geq 0$, and we can prove $P(0)$ and $P(n) \Longrightarrow P(n+1)$ for all $n \neq 3$, then we obtain $P(0)$, $P(1)$, $P(2)$, $P(3)$, but not any of $P(4)$, $P(5)$, $P(6)$, ...

1.8. More on the Fibonacci numbers

Recall the **Fibonacci sequence**:

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

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

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

.

Let us prove some more of its properties.

1.8.1. The addition theorem

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

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

Proof. Can you induct on two variables at the same time? Yes, but it's somewhat of a mess (you have to "nest" an induction inside another). Fortunately, we don't need to do this here. It suffices to induct on one variable.

Let us induct on n. To this purpose, for every integer $n \geq 0$, we define the statement $P(n)$ to be

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

(Note that $P(n)$ is **not** a single equality $f_{n+m+1} = f_n f_m + f_{n+1} f_{m+1}$ for a single number m. Rather, it is a whole sequence of such equalities, one for each $m \geq 0$.)

Base case: We must prove $P(0)$. This is saying that

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

And this is true, since

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

So the base case is complete.

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

We have assumed that $P(n)$ holds. In other words,

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

We must prove that $P(n+1)$ holds. In other words, we must prove 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,

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

But the induction hypothesis $P(n)$ (applied to $m+1$ instead of m) yields

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

(and we can indeed apply $P(n)$ to $m+1$ instead of m, because the m in $P(n)$ is not our current integer m but rather an arbitrary integer ≥ 0). Comparing these two equalities, we obtain

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

So we have proved that $f_{n+1+m+1} = f_{n+1} f_m + f_{n+1+1} f_{m+1}$ for every integer $m \geq 0$. In other words, $P(n+1)$ holds. This completes the induction step. □

1.8.2. Divisibility of Fibonacci numbers

Divisibility of integers is a basic notion in number theory, which we will elaborate upon in Chapter 3. Let us already give its definition:

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 (and we write $b \vdots a$) in this case.

For example, $2 \mid 4$ and $3 \mid 12$ and $0 \mid 0$ and $5 \mid 0$. But we don't have $2 \mid 3$ or $0 \mid 5$.

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

For example, $4 \mid 8$ entails $f_4 \mid f_8$, which is saying $3 \mid 21$.

Proof of the theorem. We want to use induction. Should we induct on a ? This is fairly hopeless, since the induction step will get stuck (the condition $a \mid b$ in the induction hypothesis has nothing to do with the condition $a + 1 \mid b$ in the induction goal). Inducting on b is also hopeless for a similar reason ($a \mid b$ has nothing to do with $a \mid b + 1$).

Let us thus get more creative and introduce a new variable to induct on. The trick is to observe that the divisibility $a \mid b$ means that $b = ac$ for some integer c (and moreover, we can pick $c \geq 0$ since $a, b \geq 0$). So we can restate our theorem as follows:

Restated theorem: For any integers $a, c \geq 0$, we have $f_a \mid f_{ac}$.

Now, let us prove this restated theorem by induction on c. In other words, for each $c \geq 0$, we shall prove the statement

$$P(c) := (\text{“for any integer } a \geq 0\text{, we have } f_a \mid f_{ac}\text{”}).$$

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

$$(\text{“for any integer } a \geq 0\text{, we have } f_a \mid f_{a \cdot 0}\text{”}).$$

But this is true, since $f_{a \cdot 0} = f_0 = 0$ is divisible by everything. So the base case is complete.

Induction step: Let $c \geq 0$ be an integer. Assume that $P(c)$ holds, i.e., that

$$\text{“for any integer } a \geq 0\text{, we have } f_a \mid f_{ac}\text{” holds.}$$

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

$$\text{“for any integer } a \geq 0\text{, we have } f_a \mid f_{a(c+1)}\text{” holds.}$$

Let $a \geq 0$ be any integer. Then, the induction hypothesis (i.e., our assumption that $P(c)$ holds) yields that $f_a \mid f_{ac}$. In other words, $f_{ac} = f_a \cdot p$ for some integer

p. Consider this p. Now, we must prove that $f_a \mid f_{a(c+1)}$ holds. We have

$$\begin{aligned} f_{a(c+1)} &= f_{ac+a} = f_{ac+(a-1)+1} \\ &= \underbrace{f_{ac}}_{=f_a \cdot p} f_{a-1} + f_{ac+1} \underbrace{f_{(a-1)+1}}_{=f_a} \qquad \left(\begin{array}{c}\text{by the addition theorem,} \\ \text{applied to } n = ac \text{ and } m = a-1\end{array}\right) \\ &= f_a \cdot p f_{a-1} + f_{ac+1} f_a = f_a \cdot \underbrace{(p f_{a-1} + f_{ac+1})}_{\text{an integer}}, \end{aligned}$$

which is clearly divisible by f_a. So we have shown that $f_a \mid f_{a(c+1)}$, and thus $P(c+1)$ is proved. This completes the induction step, and thus the theorem follows.

... almost. There is a little flaw in the above proof.

We have applied the addition theorem to $n = ac$ and $m = a-1$. But the addition theorem requires $n, m \geq 0$. So we need to ensure that ac and $a-1$ are ≥ 0. For ac, this is clear. For $a-1$, however, this is false if $a = 0$ (but fortunately only in this case). So the induction step doesn't work for $a = 0$. So let us patch this gap by just proving the $a = 0$ case by hand:

We need to prove that $f_a \mid f_{a(c+1)}$ for $a = 0$. In other words, we need to prove that $f_0 \mid f_{0(c+1)}$. But this is true, since $f_{0(c+1)} = f_0$.

So here is how the induction step we did above looks like once this gap is patched:

Induction step (correct): Let $c \geq 0$ be an integer. Assume that $P(c)$ holds, i.e., that

"for any integer $a \geq 0$, we have $f_a \mid f_{ac}$" holds.

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

"for any integer $a \geq 0$, we have $f_a \mid f_{a(c+1)}$" holds.

Let $a \geq 0$ be any integer. Then, the induction hypothesis (i.e., our assumption that $P(c)$ holds) yields that $f_a \mid f_{ac}$. In other words, $f_{ac} = f_a \cdot p$ for some integer p. Consider this p. Now, we must prove that $f_a \mid f_{a(c+1)}$ holds.

We are in one of the following two cases:

Case 1: We have $a = 0$.

Case 2: We have $a \neq 0$.

Consider Case 1. In this case, $a = 0$. Thus, $f_a \mid f_{a(c+1)}$ holds since both a and $a(c+1)$ are 0.

Now, consider Case 2. In this case, $a \neq 0$. Hence, $a \geq 1$ (since a is a nonnegative integer). Thus, $a-1 \geq 0$. Also, $ac \geq 0$. Now,

$$\begin{aligned} f_{a(c+1)} &= f_{ac+a} = f_{ac+(a-1)+1} \\ &= \underbrace{f_{ac}}_{=f_a \cdot p} f_{a-1} + f_{ac+1} \underbrace{f_{(a-1)+1}}_{=f_a} \qquad \left(\begin{array}{c}\text{by the addition theorem,} \\ \text{applied to } n = ac \text{ and } m = a-1\end{array}\right) \\ &= f_a \cdot p f_{a-1} + f_{ac+1} f_a = f_a \cdot \underbrace{\left(p f_{a-1} + f_{ac+1}\right)}_{\text{an integer}}, \end{aligned}$$

which is clearly divisible by f_a. So we have shown that $f_a \mid f_{a(c+1)}$.

Thus, in both cases, we have proved that $f_a \mid f_{a(c+1)}$. Hence, $P(c+1)$ is proved. This completes the induction step, and thus the theorem follows. □

1.8.3. Binet's formula

If we want to compute $f_{1\,000\,000}$, we must first compute $f_0, f_1, f_2, \ldots, f_{999\,999}$, because we only have a recursive formula for the Fibonacci numbers. Can we do better? Can we find an **explicit** formula for the Fibonacci numbers, i.e., a formula for f_n that does not rely on earlier values?

Yes, the so-called **Binet's formula**:

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

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

Then,

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

Some remarks:

- The number φ is called the **golden ratio**; the number ψ is known as its **conjugate**. The two numbers φ and ψ are the roots of the quadratic equation $x^2 = x + 1$.
- The numbers f_n are integers, and yet Binet's formula expresses them through the irrational numbers φ and ψ. Beware of computing f_n numerically using this formula.
- As n grows large, ψ^n approaches 0, whereas φ^n grows exponentially. So f_n also grows exponentially, and with growth rate $\varphi \approx 1.618\ldots$.
- Where does this formula come from? One answer is "linear algebra", specifically "eigenvalues of a 2 × 2-matrix". Alas, this is not the course for this.

Attempt at a proof of Binet's formula. We induct on n:

Base case: For $n = 0$, we must prove that

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

But this is true because both sides are 0.

Induction step: Let $n \geq 0$ be an integer.

Assume (as the induction hypothesis) that Binet's formula holds for n. We must prove that it holds for $n+1$ as well.

So we must prove that

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

If $n = 0$, then this is easy. For $n \geq 1$, the recurrent equation for the Fibonacci numbers yields

$$\begin{aligned} f_{n+1} &= f_n + f_{n-1} \\ &= \frac{\varphi^n - \psi^n}{\sqrt{5}} + f_{n-1} \qquad \text{(by the induction hypothesis)}. \end{aligned}$$

We are stuck: The induction hypothesis only tells us about f_n, not about f_{n-1}. Metaphorically, the n-th domino does not kick over the $(n+1)$-st one, so the cascade doesn't happen.

Thus, the principle of induction (in the form we are applying it) is not strong enough to complete this proof.

Next time, we will see a stronger version of it ("strong induction"). □

1.9. Strong induction

1.9.1. Reminder on regular induction

Recall the (original) principle of mathematical induction:

> **Theorem 1.9.1** (Principle of Induction)**.** Let b be an integer. Let $P(n)$ be a statement defined for each $n \geq b$. Assume that:
>
> 1. "**Base case**": The statement $P(b)$ holds.
>
> 2. "**Induction step**": For each integer $n \geq b$, the implication $P(n) \Longrightarrow P(n+1)$ holds.
>
> Then, the statement $P(n)$ holds for every integer $n \geq b$.

We can restate this theorem a bit by renaming the n in the induction step as $n-1$:

> **Theorem 1.9.2** (Principle of Induction, restated)**.** Let b be an integer. Let $P(n)$ be a statement defined for each $n \geq b$. Assume that:
>
> 1. "**Base case**": The statement $P(b)$ holds.
>
> 2. "**Induction step**": For each integer $n > b$, the implication $P(n-1) \Longrightarrow P(n)$ 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

$$\begin{aligned} P(b) &\Longrightarrow P(b+1), \\ P(b+1) &\Longrightarrow P(b+2), \\ P(b+2) &\Longrightarrow P(b+3), \\ &\ldots. \end{aligned}$$

We can climb up this latter to reach any $P(n)$. 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's falling.

1.9.2. Strong induction

Now, assume that the $b+2$-domino (i.e., $P(b+2)$) falls not from the impact of $P(b+1)$, 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 $P(b+1) \Longrightarrow P(b+2)$, we could just as well prove the implication

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

Likewise, we could replace the implication $P(b+2) \Longrightarrow P(b+3)$ by the implication

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

More generally, for each $n > b$, instead of proving the implication $P(n-1) \Longrightarrow P(n)$, we can get by proving only the weaker implication

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

(so that the domino $P(n)$ is tipped over by the combined force of all previous dominos, not just the one directly on its left).

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 statement defined for each $n \geq b$. Assume that:

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

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

   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 in that their induction step has a stronger induction hypothesis: Instead of only assuming $P(n-1)$, it now assumes $P(b)$ AND $P(b+1)$ AND $P(b+2)$ AND $\cdots$ AND $P(n-1)$. Thus, you can use not only $P(n-1)$ but also all the previous P's. In a sense, strong induction is "induction with a long memory".

Befoer we see an example of a strong induction proof, let me explain how strong induction works. Let's say you have proved a statement $P(n)$ for all $n \geq 0$ by strong induction. Thus,

- you have proved $P(0)$ (this is the base case);
- you have proved the implication $P(0) \Longrightarrow P(1)$ (this is the induction step for $n = 1$), and thus you conclude that $P(1)$ holds (since $P(0)$ holds);
- you have proved the implication $(P(0) \text{ AND } P(1)) \Longrightarrow P(2)$ (this is the induction step for $n = 2$), and thus you conclude that $P(2)$ holds (since $P(0)$ and $P(1)$ hold);
- you have proved the implication $(P(0) \text{ AND } P(1) \text{ AND } P(2)) \Longrightarrow P(3)$ (this is the induction step for $n = 3$), and thus you conclude that $P(3)$ holds (since $P(0)$ and $P(1)$ and $P(2)$ hold);
- and so on.

1.9.3. Example: Proof of Binet's formula

Let us prove Binet's formula using strong induction.

Proof of Binet's formula. We strongly induct on n (i.e., we use strong induction on n).

Base case: As above, we check that the formula holds for $n = 0$.

Induction step: Let $n > 0$ be an integer.

We assume that Binet's formula holds for 0, for 1, for 2, and so on, all the way up to $n-1$. (In other words, we assume that $f_k = \frac{\varphi^k - \psi^k}{\sqrt{5}}$ holds for all $k \in \{0, 1, \ldots, n-1\}$.)

We have to prove that Binet's formula also holds for n. In other words, we have to prove that $f_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}$.

We assumed that Binet's formula holds for $n-1$. In other words, $f_{n-1} = \frac{\varphi^{n-1} - \psi^{n-1}}{\sqrt{5}}$.

We assumed that Binet's formula holds for $n-2$. In other words, $f_{n-2} = \frac{\varphi^{n-2} - \psi^{n-2}}{\sqrt{5}}$.

The recursive definition of the Fibonacci numbers yields

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

In other words, Binet's formula holds for n. Right?

......

There is a problem: The formula $f_n = f_{n-1} + f_{n-2}$ holds only for $n \geq 2$ (at least the way we defined the Fibonacci numbers). So the above argument does not work for $n = 1$. Moreover, our use of the induction hypothesis for $n-2$ (giving us $f_{n-2} = \frac{\varphi^{n-2} - \psi^{n-2}}{\sqrt{5}}$) also does not work for $n = 1$, because $n-2$ is not one of the numbers $0, 1, \ldots, n-1$ in this case. Actually, f_{n-2} doesn't even makes for $n = 1$, unless we define f_{-1}.

So we need to treat the case $n = 1$ separately. (All the remaining cases $n = 2, 3, 4, \ldots$ work as claimed, since $n-1$ and $n-2$ belong to the list $0, 1, \ldots, n-1$ in those cases.)

Let's do it. We just need to check that Binet's formula holds for $n = 1$. In other words, we need to check that $f_1 = \frac{\varphi^1 - \psi^1}{\sqrt{5}}$. This is direct verification:

$f_1 = 1$ and

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

So Binet's formula holds for $n = 1$. Now the induction step is really complete, and Binet's formula is proved. □

Let us summarize: We have used strong induction in our above proof, because the "extra memory" in the induction step allowed us to express not just f_{n-1} but also f_{n-2}.

Note that we have had to handle the two cases $n = 0$ and $n = 1$ by hand. The $n = 0$ case was our base case. The $n = 1$ case was part of the induction step, but still had to be singled out because we could not go two steps back from it. So it is a "second base case", although de-jure part of the induction step.

1.9.4. Baseless strong induction

You can actually reformulate the Principle of Strong Induction in a way that does not require a de-jure base case at all:

> **Theorem 1.9.4** (Principle of Strong Induction, restated)**.** Let b be an integer. Let $P(n)$ be a statement defined for each $n \geq b$. Assume that:
>
> 1. "**Induction step**": For each integer $n \geq b$, the implication
>
> $$(P(b) \text{ AND } P(b+1) \text{ AND } P(b+2) \text{ AND } \cdots \text{ AND } P(n-1)) \Longrightarrow P(n)$$
>
>   holds.
>
> Then, the statement $P(n)$ holds for every integer $n \geq b$.

How does this restated principle work without a base case? Easy: We have just repackaged the base case into the induction step. Indeed, the induction step now allows for $n = b$ (since it says "$n \geq b$" instead of "$n > b$"). For $n = b$, the implication

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

becomes

$$\underbrace{(P(b) \text{ AND } P(b+1) \text{ AND } P(b+2) \text{ AND } \cdots \text{ AND } P(b-1))}_{\substack{\text{a conjunction of 0 statements,} \\ \text{i.e., a statement that is automatically true}}} \Longrightarrow P(b),$$

so to prove this implication means to prove $P(b)$ unconditionally, and that's exactly what the base case would do. So we have not magically removed the need for proving $P(b)$; we just have folded it into the induction step. So the baseless form of strong induction is equivalent to the usual form, just stated a little bit more cleanly.

1.9.5. Example: Prime factorization exist

Here is another example of a strong induction proof, coming from number theory. We need two definitions:

Definition 1.9.5. Let b be an integer. A **divisor** of b means an integer a that divides b.

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

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 you will show later.

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

Here and in the following, I understand an empty product (i.e., a product of no numbers whatsoever) to be 1. Thus, the theorem holds for 1 (since 1 is a product of no 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 (2 itself).

How do we prove the theorem in general?

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. (We use the original variant, with a base case.)

Base case: $P(1)$ is true, since 1 is a product of finitely many primes (namely, 0 primes).

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

$$(P(1) \text{ AND } P(2) \text{ AND } P(3) \text{ AND } \cdots \text{ AND } P(n-1)) \Longrightarrow P(n).$$

So we assume that $P(1)$ AND $P(2)$ AND $P(3)$ 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 of n that is neither 1 nor n.

Consider Case 1 first. In this case, n is prime. Thus, n is a product of finitely many primes (just one). Thus, $P(n)$ holds in Case 1.

Now, consider Case 2. In this case, there is a positive divisor d of n that is neither 1 nor n. Consider this d.

Since d is a positive divisor of n, we have $1 \leq d \leq n$ (strictly speaking, this needs proof; see later). Since d is neither 1 nor n, we can improve this to $1 < d < n$. In particular, this yields that d is one of the numbers $1, 2, \ldots, n-1$. Hence, $P(d)$ holds (since we assumed that $P(1)$ AND $P(2)$ AND $P(3)$ AND $\cdots$ AND $P(n-1)$ holds). In other words, d is a product of primes. That is, we can write d as

$$d = p_1 p_2 \cdots p_k \qquad \text{for some primes } p_1, p_2, \ldots, p_k.$$

Consider these $p_1, p_2, \ldots, p_k$.

Since d is a divisor of n, the ratio $\frac{n}{d}$ is an integer. This integer $\frac{n}{d}$ is positive (since n and d are positive) and is $< n$ (since $d > 1$). Hence, it is one of the numbers $1, 2, \ldots, n-1$. Therefore, $P\left(\frac{n}{d}\right)$ holds (since we assumed that $P(1)$ AND $P(2)$ AND $P(3)$ AND $\cdots$ AND $P(n-1)$ holds). In other words, $\frac{n}{d}$ is a product of primes. That is, we can write $\frac{n}{d}$ as

$$\frac{n}{d} = q_1 q_2 \cdots q_\ell \qquad \text{for some primes } q_1, q_2, \ldots, q_\ell.$$

Consider these $q_1, q_2, \ldots, q_\ell$.

Now,

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

This shows that n is a product of primes. In other words, $P(n)$ holds.

Thus we have proved $P(n)$ in both Case 1 and Case 2. This completes the induction step, and the theorem is proved. □

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

Another example for 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: 3
4 cents	no
5 cents	yes: 5
6 cents	yes: $3+3$
7 cents	no
8 cents	yes: $3+5$
9 cents	yes: $3+3+3$
10 cents	yes: $5+5$
11 cents	yes: $3+3+5$
12 cents	yes: $3+3+3+3$
13 cents	yes: $3+5+5$
...	...

Experimentally, we seem to observe that any denomination ≥ 8 cents can be paid. Why?

It suffices to show that 8 cents, 9 cents and 10 cents can be paid, because then (by adding a 3-cent coin) we can also pay 11 cents, 12 cents and 13 cents, and therefore (by adding another 3-cent coin) we can also pay 14 cents, 15 cents and 16 cents, and so on.

Let us formalize this argument as an 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 also holds 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 $n = 10 = 3 \cdot 0 + 5 \cdot 2$.

Let us now consider Case 3. In this case, we have $n \geq 11$. Hence, $n - 3 \geq 8$. This shows that $n - 3$ is one of the numbers $8, 9, \ldots, n - 1$. Thus, we can apply the induction hypothesis to $n - 3$. This shows that $n - 3$ cents can be paid with 3-cent and 5-cent coins. In other words,

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

Using these c, d, we thus have

$$\begin{aligned} n &= 3 + 3c + 5d \\ &= 3\left(c + 1\right) + 5d. \end{aligned}$$

This shows that n cents can be paid with 3-cent and 5-cent coins. Thus, the proposition is true for n, and the induction step is complete. □

Note that the above proof had one "de-jure base case" (the case $n = 8$) and two "de-facto base cases" (the cases $n = 9$ and $n = 10$, which were formally part of the induction step but had to be treated separately because $n - 3$ would be too small). If we had used baseless strong induction, all three of them would become "de-facto base cases".

2. Sums and products

2.1. Finite sums

Previously, we have seen sums such as

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

Such sums can be tricky to decipher: It requires spotting the pattern and extending it. Now let me introduce a notation for such sums that makes them both easier to decipher and unambiguous:

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

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

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 is defined to be 0.

Examples:

$$\sum_{k=6}^{11} k = 6+7+8+9+10+11 = 51;$$

$$\sum_{k=6}^{11} \frac{1}{k} = \frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\frac{1}{9}+\frac{1}{10}+\frac{1}{11};$$

$$\sum_{k=6}^{11} k^k = 6^6+7^7+8^8+9^9+10^{10}+11^{11};$$

$$\sum_{k=6}^{6} k = 6;$$

$$\sum_{k=6}^{4} k = 0 \qquad \text{(an empty sum)};$$

$$\sum_{k=6}^{5} k = 0 \qquad \text{(an empty sum)};$$

$$\sum_{k=0}^{n-1} q^k = q^0+q^1+\cdots+q^{n-1} \qquad \text{(where } q \text{ is any number and } n \in \mathbb{N}\text{)};$$

$$\begin{aligned}\sum_{k=0}^{n-1} x^k y^{n-1-k} &= x^0y^{n-1}+x^1y^{n-2}+x^2y^{n-3}+\cdots+x^{n-3}y^2+x^{n-2}y^1+x^{n-1}y^0\\ &= y^{n-1}+xy^{n-2}+x^2y^{n-3}+\cdots+x^{n-3}y^2+x^{n-2}y+x^{n-1}\\ &= x^{n-1}+x^{n-2}y+x^{n-3}y^2+\cdots+x^2y^{n-3}+xy^{n-2}+y^{n-1}\\ &\qquad \text{(for any numbers } x,y \text{ and any } n \in \mathbb{N}\text{)}.\end{aligned}$$

Thus our theorem from a while ago can be rewritten in the following cleaner and simpler form:

Theorem 2.1.2. Let x and y be any two numbers. Then, for any integer $n \geq 0$, we have

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

The variable k is not set in stone. You can just as well use any other letter or symbol that is not otherwise occupied. For example, you can rewrite $\sum\limits_{k=u}^{v} a_k$ as $\sum\limits_{i=u}^{v} a_i$ or as $\sum\limits_{x=u}^{v} a_x$ or as $\sum\limits_{\spadesuit=u}^{v} a_{\spadesuit}$, but please do not write $\sum\limits_{u=u}^{v} a_u$.

A couple more examples: For any $n \in \mathbb{N}$, we have

$$\sum_{k=1}^{n} k = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \qquad \text{(by Little Gauss)};$$
$$\sum_{k=1}^{n} k^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6};$$
$$\sum_{k=1}^{n} 1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = n \cdot 1 = n;$$
$$\begin{aligned}\sum_{k=1}^{n} (2k-1) &= (2 \cdot 1 - 1) + (2 \cdot 2 - 1) + (2 \cdot 3 - 1) + \cdots + (2 \cdot n - 1) \\ &= 1 + 3 + 5 + \cdots + (2n-1) \\ &= (\text{sum of the first } n \text{ odd positive integers}).\end{aligned}$$

Let us compute this last sum. We will use the following "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. Indeed, without using finite sum notation, this can be rewritten as
$$\begin{aligned}&(a_u - b_u) + (a_{u+1} - b_{u+1}) + \cdots + (a_v - b_v) \\ &= (a_u + a_{u+1} + \cdots + a_v) - (b_u + b_{u+1} + \cdots + b_v).\end{aligned}$$

- 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, a_k. Indeed, this is saying that
$$\lambda a_u + \lambda a_{u+1} + \cdots + \lambda a_v = \lambda (a_u + a_{u+1} + \cdots + a_v).$$

Rules like these are dime a dozen, and you should be able to come up with them as needed. (See the references in the notes for a list.)

Now we compute our sum:

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

As another illustration of our "finite sum calculus", we can rewrite Gauss's proof of the Little Gauss formula

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

using the finite sum notation. We will need three new rules this time:

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

- We have
$$\sum_{k=u}^{v} a_k = \sum_{k=u}^{v} a_{u+v-k}$$
for any integers u, v and any numbers a_k. Rewritten without finite sum notation, this is saying that
$$a_u + a_{u+1} + \cdots + a_v = a_v + a_{v-1} + \cdots + a_u.$$
The two sums in this equation have the same addends in opposite order. So our rule is just saying that any sum can be reversed (i.e., its addends can be put in opposite order) without changing its value. This rule is called "substituting $u + v - k$ for k in the sum" or just "turning the sum upside-down".

- For any integers $u \leq v$ and any number λ, we have
$$\sum_{k=u}^{v} \lambda = \left(v - u + 1\right)\lambda.$$

Now, Gauss's proof takes the following shape:

$$\begin{aligned} 2\sum_{k=1}^{n} k &= \sum_{k=1}^{n} k + \sum_{k=1}^{n} k \\ &= \sum_{k=1}^{n} k + \sum_{k=1}^{n} \left(n + 1 - k\right) \qquad \left(\begin{array}{c}\text{here, we substituted } n+1-k \\ \text{for } k \text{ in the second sum}\end{array}\right) \\ &= \sum_{k=1}^{n} \underbrace{\left(k + \left(n + 1 - k\right)\right)}_{=n+1} = \sum_{k=1}^{n} \left(n+1\right) = n \cdot \left(n+1\right). \end{aligned}$$

Division by 2 thus yields $\sum_{k=1}^{n} k = \frac{n \cdot (n+1)}{2}$, qed.

We have now found closed-form expressions for several sums. Not every sum has a closed-form expression. For example, there is no way to simplify $\sum\limits_{k=1}^{n} \dfrac{1}{k}$ or $\sum\limits_{k=1}^{n} k^k$.

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 numbers 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.

There are many similarities between finite sums $\sum\limits_{k=u}^{v} a_k$ and integrals $\int\limits_u^v f(x)\,dx$. There are some differences, though: $\sum\limits_{k=u}^{u} a_k = a_u$ (often nonzero) but $\int\limits_u^u f(x)\,dx = 0$. Also, $\sum\limits_{k=u}^{u-1} a_k = 0$ but $\int\limits_u^{u-1} f(x)\,dx \neq 0$ usually.

Two more rules for finite sums:

- The "splitting-off rule": For any integers $u \leq v$ and any numbers $a_u, a_{u+1}, \ldots, a_v$, we have

$$\begin{aligned}\sum_{k=u}^{v} a_k &= a_u + \sum_{k=u+1}^{v} a_k \qquad \text{(here, we "split off" the first addend)} \\ &= \sum_{k=u}^{v-1} a_k + a_v \qquad \text{(here, we "split off" the last addend)}.\end{aligned}$$

  This is very useful for induction proofs.

- More generally, a finite sum $\sum\limits_{k=u}^{v} a_k$ 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 $u \leq w \leq v$ and any numbers a_k. Without summation signs, this is just saying that

$$a_u + a_{u+1} + \cdots + a_v = (a_u + a_{u+1} + \cdots + a_w) + (a_{w+1} + a_{w+2} + \cdots + a_v).$$

Finite sum notation, in the form above, is helpful when the summation index is running over an integer interval (i.e., all integers from u to v for given u, v).

More general versions of finite sums can be used to sum over other sets. For example,

$$\sum_{k\in\{1,2,\ldots,n\} \text{ is even}} k = 2+4+6+\cdots+m,$$

where m is the largest even element of $\{1,2,\ldots,n\}$. (This m is actually $2\left\lfloor \frac{n}{2} \right\rfloor$.) See the notes and the references therein for more details.

See also the notes for a bunch of exercises.

2.2. Finite products

Finite products are just like finite sums, except that they rely on multiplication instead of addition:

> **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
>
> $$a_u a_{u+1} \cdots a_v.$$
>
> It is called the **product of the numbers a_k where k ranges from u to v**. When $v < u$, it is called **empty** and defined to be 1.

For example:

$$\prod_{k=6}^{11} k = 6\cdot 7\cdot 8\cdot 9\cdot 10\cdot 11 = 332\,640;$$

$$\prod_{k=6}^{11} \frac{1}{k} = \frac{1}{6}\cdot\frac{1}{7}\cdot\frac{1}{8}\cdot\frac{1}{9}\cdot\frac{1}{10}\cdot\frac{1}{11} = \frac{1}{332\,640};$$

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

$$\prod_{k=1}^{n} a = \underbrace{aa\cdots a}_{n \text{ times}} = a^n \qquad \text{for any number } a \text{ and any } n \in \mathbb{N};$$

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

$$\text{for any number } a \text{ and any } n \in \mathbb{N}.$$

In a finite product $\prod\limits_{k=u}^{v} a_k$, the k is called the **product index** or the **running index**, and the symbol $\prod$ is called the **product sign**. The numbers a_k are called the **factors** of the product. Other terminology is analogous to the corresponding terminology for sums. Almost all rules for finite sums have analogues for finite products. For example:

- The "splitting-off rule": For any integers $u \leq v$ and any numbers $a_u, a_{u+1}, \ldots, a_v$, we have

$$\begin{aligned} \prod_{k=u}^{v} a_k &= a_u \cdot \prod_{k=u+1}^{v} a_k && \text{(here, we "split off" the first factor)} \\ &= \prod_{k=u}^{v-1} a_k \cdot a_v && \text{(here, we "split off" the last factor)} . \end{aligned}$$

  This is very useful for induction proofs.

2.3. Factorials

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

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

$$n! = 1 \cdot 2 \cdot \cdots \cdot n.$$

This is the product of the first n positive integers.

For example,

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

Note the following:

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

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

Proof. We have

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

□

See the end of §2.3 for several exercises on products and factorials.

2.4. Binomial coefficients: Definition

We are now ready to introduce the most important family of numbers in mathematics.

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

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

  $$\dbinom{n}{k} := \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}$$

  (where the numerator is the product of k "consecutive numbers", the largest of which is n).

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

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

The number $\dbinom{n}{k}$ 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

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

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

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

$$\binom{-1}{k} = \frac{\left(-1\right)\left(-2\right)\left(-3\right)\cdots\left(-k\right)}{k!} = \frac{\left(-1\right)^k \cdot \left(1 \cdot 2 \cdot \cdots \cdot k\right)}{1 \cdot 2 \cdot \cdots \cdot k} = \left(-1\right)^k.$$

Let us tabulate the values of $\binom{n}{k}$ for nonnegative integers n and k:

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$
$n=0$	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

.

The first thing that might catch your attention here is the wall of zeroes in the upper-right half of the table. This has a simple reason:

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

Proof. We have

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

since the product $n\,(n-1)\,(n-2)\cdots(n-k+1)$ contains the factor $n-n=0$. So $\dbinom{n}{k} = 0$.

For example,

$$\binom{2}{4} = \frac{2\cdot 1\cdot 0\cdot(-1)}{4!} = 0.$$

$\square$

Warning: If $n \notin \mathbb{N}$, then $k > n$ does not imply $\dbinom{n}{k} = 0$. For example,

$$\binom{1.5}{3} = \frac{1.5\cdot 0.5\cdot(-0.5)}{3!} \neq 0.$$

The proposition we just proved suggests that we stop tabulating the coefficients $\dbinom{n}{k}$ with $k > n$, and focus on the ones with $k \leq n$. It makes more sense to arrange these remaining coefficients in a triangle:

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

This table is known as **Pascal's triangle**, and has many wonderful properties:

- **Pascal's identity, aka the recurrence of the BCs (= binomial coefficients):** For any numbers n and k, we have
$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$
- **Symmetry of binomial coefficients:** For any $n \in \mathbb{N}$ and any k, we have
$$\binom{n}{k} = \binom{n}{n-k}.$$
- We have $\dbinom{n}{n} = 1$ for each $n \in \mathbb{N}$.
- **Integrality of binomial coefficients:** For any $n \in \mathbb{Z}$ and any k, we have $\dbinom{n}{k} \in \mathbb{Z}$.

Let us prove these facts now, starting with the most important one.

2.5. Binomial coefficients: Properties

2.5.1. Pascal's identity

Theorem 2.5.1 (Pascal's identity)**.** For any numbers n and k, we have
$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Proof. 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. (So $k \notin \mathbb{N}$.)

Let us first consider Case 1. Here, k is a positive integer. Hence, both k and $k-1$ belong to $\mathbb{N}$. Thus, the definition of BCs yields the three formulas
$$\begin{aligned}
\binom{n}{k} &= \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!};\\
\binom{n-1}{k-1} &= \frac{(n-1)(n-2)(n-3)\cdots((n-1)-(k-1)+1)}{(k-1)!}\\
&= \frac{(n-1)(n-2)(n-3)\cdots(n-k+1)}{(k-1)!};\\
\binom{n-1}{k} &= \frac{(n-1)(n-2)(n-3)\cdots((n-1)-k+1)}{k!}\\
&= \frac{(n-1)(n-2)(n-3)\cdots(n-k)}{k!}.
\end{aligned}$$

Setting $a := (n-1)(n-2)(n-3)\cdots(n-k+1)$, these three formulas can be rewritten as

$$\begin{aligned} \binom{n}{k} &= \frac{na}{k!}; \\ \binom{n-1}{k-1} &= \frac{a}{(k-1)!}; \\ \binom{n-1}{k} &= \frac{a(n-k)}{k!}. \end{aligned}$$

So the formula we are proving – that is, the formula

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

– simplifies to

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

Multiplying this by $k!$, we transform it into

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

Since $\dfrac{k!}{(k-1)!} = k$ (by the factorial recurrence $k! = (k-1)! \cdot k$), we can simplify this further to

$$na = a \cdot k + a(n-k),$$

which is obvious. So our claim is proved in Case 1.

Now, consider Case 2. In this case, $k = 0$. Hence, our claim

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

rewrites as

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

which is obvious.

Finally, consider Case 3. In this case, k is neither a positive integer nor 0. Hence, $k \notin \mathbb{N}$. Thus, $k-1 \notin \mathbb{N}$. Therefore, our claim

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

is true.

So we are done in all three cases, and the theorem is proved. □

Pascal's identity is highly useful for proving properties of $\binom{n}{k}$ by induction on n (at least when $n \in \mathbb{N}$). Note that it is true not just for $n \in \mathbb{N}$, but for all numbers n. For example,

$$\binom{-3}{5} = \binom{-4}{4} + \binom{-4}{5} \qquad \text{and}$$
$$\binom{3.2}{2} = \binom{2.2}{1} + \binom{2.2}{2}.$$

2.5.2. The factorial formula

Binomial coefficients $\binom{n}{k}$ make sense for arbitrary numbers n and k. But there is a particularly simple expression in the case when $n \in \mathbb{N}$ and $k \in \{0, 1, \ldots, n\}$:

Theorem 2.5.2 (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 BCs yields

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

Since

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

this rewrites as

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

□

Warning: The factorial formula $\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$ does **not** hold if n is negative or non-integer. So it is less general than the definition of BCs.

2.5.3. The symmetry of BCs

Theorem 2.5.3 (symmetry of BCs)**.** Let $n \in \mathbb{N}$, and let k be any number. Then,

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

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.

Let us first consider Case 1. In this csae, $k \in \{0, 1, \ldots, n\}$, and thus $n - k \in \{0, 1, \ldots., n\}$. Therefore, we can apply the factorial formula to obtain

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

which clearly yields $\binom{n}{k} = \binom{n}{n-k}$.

Now, consider Case 2, in which $k < 0$. Hence, $k \notin \mathbb{N}$ and therefore $\binom{n}{k} = 0$ by definition. But $\binom{n}{n-k} = 0$ by the first proposition we proved about BCs (since $n - k > n$ (since $k < 0$)). So again $\binom{n}{k} = \binom{n}{n-k}$.

Case 3 is similar to Case 2, but k and $n - k$ switch roles.

Case 4 is even easier, since in that case both $\binom{n}{k}$ and $\binom{n}{n-k}$ are 0 by definition.

So we are done in all four cases. □

Corollary 2.5.4. For any $n \in \mathbb{N}$, we have $\binom{n}{n} = 1$.

Proof. Applying the symmetry theorem to $k = n$, we get

$$\binom{n}{n} = \binom{n}{n-n} = \binom{n}{0} = 1.$$

□

Warning: Neither the theorem nor the corollary hold when n is negative or non-integer. For instance, $\binom{-1}{-1}$ is 0, not 1.

2.5.4. Pascal's triangle consists of integers

Theorem 2.5.5. For any $n \in \mathbb{N}$ and any number k, we have $\dbinom{n}{k} \in \mathbb{N}$.

Proof. We induct on n.

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

$$\binom{0}{k} = \begin{cases} 1, & \text{if } k = 0; \\ 0, & \text{if } k \neq 0 \end{cases} \in \mathbb{N}.$$

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

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

Our goal is to prove that the theorem holds for n. In other words, we must prove that

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

Let's do this: For any number k, Pascal's identity yields

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

So the induction step is complete. The theorem is proved. □

There is a different proof of the theorem, one which really explains what $\dbinom{n}{k}$ is. This proof proceeds through the following result:

Theorem 2.5.6 (combinatorial interpretation of BCs)**.** Let $n \in \mathbb{N}$, and let k be any number. Let A be any n-element set (e.g., the set $\{1, 2, \ldots, n\}$). Then,

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

Example 2.5.7. Let $n = 4$ and $k = 2$ and $A = \{1, 2, 3, 4\}$. Then, the 2-element subsets of A are

$$\underbrace{\{1,2\}}_{\substack{=\{2,1\} \\ =\{1,2,1\}}}, \quad \{3,4\}, \quad \{1,3\}, \quad \{2,4\}, \quad \{1,4\}, \quad \{2,3\}.$$

So there are 6 of them. This matches the claim of the theorem, because $\dbinom{4}{2} = 6$.

We will prove the theorem later in this course (Chapter 4), as we learn more about counting. Note that these k-element subsets are also known as **combinations without replacement**.

2.5.5. Upper negation

Theorem 2.5.8 (Upper negation formula)**.** 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 obvious.

Remains to handle the case $k \in \mathbb{N}$. In this case, the definition of BCs yields

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

and

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

Comparing these, we find

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

qed. □

Corollary 2.5.9. For any $n \in \mathbb{Z}$ and any number k, we have $\dbinom{n}{k} \in \mathbb{Z}$.

Proof. When $n \geq 0$, this has already been proved.

When $k \notin \mathbb{N}$, this is obvious (since $\dbinom{n}{k} = 0$).

In the remaining case, use upper negation (details left to the reader). □

2.5.6. Finding Fibonacci numbers in Pascal's triangle

Theorem 2.5.10. For any $n \in \mathbb{N}$, the Fibonacci number f_{n+1} is

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

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

$$\begin{aligned} f_8 &= \binom{7-0}{0} + \binom{7-1}{1} + \binom{7-2}{2} + \cdots + \binom{7-7}{7} \\ &= 1 + 6 + 10 + 4 + 0 + 0 + 0 = 21. \end{aligned}$$

We will prove this theorem later on, in Chapter 6 (on enumerative combinatorics).

2.6. The binomial formula

The BCs are called BCs because they are the coefficients in the **binomial formula**:

Theorem 2.6.1 (binomial formula, aka the binomial theorem)**.** Let a and b be any two numbers, and let $n \in \mathbb{N}$. Then,

$$\begin{aligned} (a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\ &= \binom{n}{0} a^0 b^n + \binom{n}{1} a^1 b^{n-1} + \binom{n}{2} a^2 b^{n-2} + \cdots + \binom{n}{n} a^n b^0 \\ &= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k. \end{aligned}$$

Example 2.6.2. For $n = 4$, this says that

$$\begin{aligned} (a+b)^4 &= \binom{4}{0} a^0 b^4 + \binom{4}{1} a^1 b^3 + \binom{4}{2} a^2 b^2 + \binom{4}{3} a^3 b^1 + \binom{4}{4} a^4 b^0 \\ &= b^4 + 4ab^3 + 6a^2b^2 + 4a^3b + a^4 \\ &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4. \end{aligned}$$

Likewise, for $n = 2$, this says that

$$(a+b)^2 = a^2 + 2ab + b^2.$$

Proof of the binomial formula. It suffices to prove the identity

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

(since the other two follow from it easily). We will prove this identity by induction on n:

Base case: This identity holds for $n=0$, since

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

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

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

We must prove that this identity also holds for $n+1$. In other words, we must prove that

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

We have

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)^n \cdot (a+b) \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right) \cdot (a+b) \qquad \text{(by the IH)} \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right) \cdot a + \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right) \cdot b \\
&= \sum_{k=0}^{n} \binom{n}{k} \underbrace{a^k b^{n-k} a}_{=a^{k+1} b^{n-k}} + \sum_{k=0}^{n} \binom{n}{k} a^k \underbrace{b^{n-k} b}_{=b^{n-k+1}} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1}.
\end{aligned}$$

On the other hand,

$$\sum_{k=0}^{n+1} \underbrace{\binom{n+1}{k}}_{\substack{=\binom{n}{k-1}+\binom{n}{k} \\ \text{(by Pascal's identity)}}} a^k b^{n+1-k}$$

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

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

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

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

Comparing these two equalities, we see that the second sums on their RHSs are the same:

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

(since $n - k + 1 = n + 1 - k$). If we can show that the first sums are also the same, then we will conclude that the whole RHSs are equal, and so the LHSs must also be equal, and this will finish our induction step.

So our goal is now to prove that the first sums are the same, i.e., that

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

But both of these sums contain the exact same addends if you write them out:

$$\binom{n}{0} a^1 b^n + \binom{n}{1} a^2 b^{n-1} + \binom{n}{2} a^3 b^{n-2} + \cdots + \binom{n}{n} a^{n+1} b^0.$$

So they are equal.

This argument can be made more rigorously using a summation rule called **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 integral formula

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

When we use the above formula

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

to rewrite a sum $\sum\limits_{k=u}^{v} c_k$ as $\sum\limits_{k=u+\delta}^{v+\delta} c_{k-\delta}$, we say that we are **substituting** $k-\delta$ for k in the sum. For example, substituting $k-1$ for k in the sum $\sum\limits_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k}$ transforms it into

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

which is exactly what we wanted.

Combining all the above, we see that

$$\begin{aligned}(a+b)^{n+1} &= \underbrace{\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k}}_{=\sum\limits_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k}} + \sum_{k=0}^{n} \binom{n}{k} a^k \underbrace{b^{n-k+1}}_{=b^{n+1-k}} \\ &= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.\end{aligned}$$

In other words, the binomial formula holds for $n+1$. This completes the induction step, and thus the binomial formula is proved. □

3. Elementary number theory

Number theory means the study of integers and similar objects.

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 $a \nmid b$ if we don't have $a \mid b$.

Example 3.1.2. (a) We have $4 \mid 12$, because $12 = 4 \cdot 3$.

(b) We have $1 \mid b$ for every integer b, since $b = 1 \cdot b$.

(c) We have $a \mid a$ for each integer a, since $a = a \cdot 1$. In particular, $0 \mid 0$.

(d) We have $a \mid 0$ for each integer a, since $0 = a \cdot 0$.

(e) An integer b satisfies $0 \mid b$ and only if $b = 0$.

Definition 3.1.3. (a) An integer n is said to be **even** if $2 \mid n$.

(b) An integer n is said to be **odd** if $2 \nmid n$.

You might know a few things about even and odd numbers: e.g..

1. an even number plus an even number is an even number;
2. an even number plus an odd number is an odd number;
3. an odd number plus an odd number is an even number.

The first of these statements is easy to prove ($2c + 2d = 2(c + d)$), but the second is trickier, and it is not clear how to prove the third (if all you have is definition of "even" and "odd"). So we need to understand divisibility better.

3.1.2. Basic properties

In the following proposition, we shall let $\operatorname{abs} x$ denote the absolute value of a real number x. This is commonly called $|x|$.

Proposition 3.1.4. Let a and b be two integers. Then:

(a) We have $a \mid b$ if and only if $\operatorname{abs} a \mid \operatorname{abs} b$.

(b) If $a \mid b$ and $b \neq 0$, then $\operatorname{abs} a \leq \operatorname{abs} b$.

(c) If $a \mid b$ and $b \mid a$, then $\operatorname{abs} a = \operatorname{abs} b$.

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

Proof. **(a)** This part is just saying that the divisibility of a and b does not depend on the signs of a and b, i.e., does not change its truth (or falsity) if we flip any of these signs. Thus, in order to prove it, we must show the following two claims:

1. We have $a \mid b$ if and only if $-a \mid b$.

2. We have $a \mid b$ if and only if $a \mid -b$.

To prove the first claim, we can argue that $a \mid b$ implies $-a \mid b$ as follows: If $a \mid b$, then there exists an integer c such that $b = ac$, and therefore $b = ac = (-a)(-c)$, which shows that $-a \mid b$. Conversely, we can argue that $-a \mid b$ implies $a \mid b$ as follows: If $-a \mid b$, then there exists an integer c such that $b = (-a)c$, and therefore $b = (-a)c = a(-c)$, which shows that $a \mid b$.

So the first claim is proved.

For the second claim, proceed similarly: We can argue that $a \mid b$ implies $a \mid -b$ as follows: If $a \mid b$, then there exists an integer c such that $b = ac$, and therefore $-b = -ac = a(-c)$, which shows that $a \mid -b$. Similarly, we can argue the converse.

Thus, both claims are proved, and part **(a)** follows.

(b) Assume that $a \mid b$ and $b \neq 0$. We must prove that $\operatorname{abs} a \leq \operatorname{abs} b$.

Set $x = \operatorname{abs} a$ and $y = \operatorname{abs} b$. So we must prove that $x \leq y$.

From $a \mid b$, we obtain $\operatorname{abs} a \mid \operatorname{abs} b$ (by part **(a)**), that is, $x \mid y$.

We have $x \geq 0$ and $y > 0$ (since $b \neq 0$).

From $x \mid y$, we see that there exists an integer z such that $y = xz$. Consider this z. If $z \leq 0$, then we would have $y = \underbrace{x}_{\geq 0}\underbrace{z}_{\leq 0} \leq 0$, contradict $y > 0$. Hence, we cannot have $z \leq 0$. Thus, $z > 0$, so that $z \geq 1$ (since z is an integer). Multiplying this inequality by x (this is allowed since $x \geq 0$), we find $xz \geq x1$. Thus, $y = xz \geq x1 = x$, that is, $x \leq y$, qed.

(c) Assume that $a \mid b$ and $b \mid a$. We must prove that $\operatorname{abs} a = \operatorname{abs} b$.

If $a = 0$, then $b = 0$ as well (since $a \mid b$) and we are done.

Similarly, we are done if $b = 0$.

It remains to handle the remaining case, which is when neither a nor b is 0. In this case, part **(b)** yields $\operatorname{abs} a \leq \operatorname{abs} b$. But part **(b)** can also be applied with the roles of a and b switched, and then it yields $\operatorname{abs} b \leq \operatorname{abs} a$. Combining these two inequalities, we find $\operatorname{abs} a = \operatorname{abs} b$.

(d) Assume that $a \mid b$. Thus, there exists an integer c such that $b = ac$. For this c, we must then have $c = \frac{b}{a}$ (since $b = ac$ and $a \neq 0$) and therefore $\frac{b}{a} = c \in \mathbb{Z}$. So we have shown that $a \mid b$ implies $\frac{b}{a} \in \mathbb{Z}$.

Conversely, $\frac{b}{a} \in \mathbb{Z}$ implies $a \mid b$ because $b = a \cdot \frac{b}{a}$. □

Theorem 3.1.5 (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 $d \mid a + b$. (In other words, a sum of two multiples of d is again a multiple of d.)

Proof. **(a)** This is because $a = a \cdot 1$.

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

From $a \mid b$, we see that there exists an integer x such that $b = ax$.

From $b \mid c$, we see that there exists an integer y such that $c = by$.

Consider these x and y.

We have

$$c = \underbrace{b}_{=ax} y = axy = a \underbrace{(xy)}_{\text{an integer}} .$$

Hence, $a \mid c$.

(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 there exists an integer c_1 such that $b_1 = a_1 c_1$.

From $a_2 \mid b_2$, we see that there exists an integer c_2 such that $b_2 = a_2 c_2$.

Now,

$$b_1 b_2 = (a_1 c_1)(a_2 c_2) = (a_1 a_2) \underbrace{(c_1 c_2)}_{\text{an integer}} .$$

This shows 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 $d \mid a + b$.

From $d \mid a$, we see that there exists an integer x such that $a = dx$.

From $d \mid b$, we see that there exists an integer y such that $b = dy$.

Now,

$$a + b = dx + dy = d \underbrace{(x + y)}_{\text{an integer}} .$$

This shows that $d \mid a + b$. □

Part **(b)** of the above theorem tells us that divisibilities can be chained together: If $a \mid b$ and $b \mid c$, then $a \mid c$. Often, such compound statements are written as chains of divisibilities: e.g., one writes "$a \mid b \mid c$" for "$a \mid b$ and $b \mid c$". More generally, the statement

$$a_1 \mid a_2 \mid \cdots \mid a_k$$

means that each of the numbers $a_1, a_2, \ldots, a_k$ divides the next (i.e., that $a_i \mid a_{i+1}$ for each i). By induction on k, it is easy to see that such a statement always entails $a_1 \mid a_k$. For instance, $3 \mid 6 \mid 18 \mid 36$, so that $3 \mid 36$.

Exercise 3.1.1. Let $a, b \in \mathbb{Z}$ such that $a \mid b$. Prove that $a^k \mid b^k$ for each $k \in \mathbb{N}$.

3.1.3. Divisibility criteria

How can you spot divisibilities between actual numbers? For small values of a, checking whether a given integer b is divisible by a can be greatly simplified using the following **divisibility criteria**:

Theorem 3.1.6. Let $b \in \mathbb{N}$. Write b in decimal notation. 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 3.1.7. Let $b = 8102$. Is $3 \mid b$? No, since the sum of the digits of b is $8 + 1 + 0 + 2 = 11$, which is not divisible by 3. Similarly, b is not divisible by 9 either.

Example 3.1.8. Let $b = 8106$. Is $3 \mid b$? Yes, since its sum of digits is $8 + 1 + 0 + 6 = 15$, which is divisible by 3. Is $9 \mid b$? No, since 15 is not divisible by 9.

Part **(c)** of the theorem is easy to prove:

- If $10 \mid b$, then the last digit of b is 0 because multiplying a number by 10 simply inserts a 0 at its end.
- If the last digit of b is 0, then $b = 10b'$ where b' is the number b with its last digit removed; therefore, $10 \mid b$.

Parts **(a)** and **(b)** are also not hard to prove. But parts **(d)** and **(e)** are tricky. We will prove them using another 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 $n \mid a - b$.

The notation for this is "$a \equiv b \bmod n$".

The notation for "a is not congruent to b modulo n" is "$a \not\equiv b \bmod n$".

Example 3.2.2. **(a)** Is $3 \equiv 7 \bmod 2$? By definition, this means that $2 \mid 3-7$, which is true (since $3-7=-4=2\cdot(-2)$). So yes, $3 \equiv 7 \bmod 2$.

(b) Is $3 \equiv 6 \bmod 2$? By definition, this means that $2 \mid 3-6$, which is false ($3-6=-3$ is odd). So $3 \not\equiv 6 \bmod 2$.

(c) We have $a \equiv b \bmod 1$ for any $a, b \in \mathbb{Z}$.

(d) Two integers a and b satisfy $a \equiv b \bmod 0$ if and only if $a = b$.

(e) For any integers a and b, we have $a + b \equiv a - b \bmod 2$, since $(a+b) - (a-b) = 2b$ is divisible by 2.

The word "modulo" should be read as something like "with respect to". Two integers a and b are congruent modulo n if and only if a equals b up to a multiple of n, i.e., if a equals b plus a multiple of n. More formally:

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

As we will soon see, congruence modulo 2 is parity: Two integers are congruent modulo 2 if and only if they are both even or both odd.

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. By the definition of congruence,

$$(a \equiv 0 \bmod n) \iff (n \mid a - 0) \iff (n \mid a).$$

□

Proposition 3.2.4. Let $n \in \mathbb{Z}$. Then:

(a) We have $a \equiv a \bmod n$ for each $a \in \mathbb{Z}$. (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 the **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 the **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 $a \equiv b \bmod m$. (For instance, if $a \equiv b \bmod 15$, then $a \equiv b \bmod 3$.)

Proof. **(a)** For each $a \in \mathbb{Z}$, we have $n \mid a - a$ (since $a - a = 0 = n \cdot 0$) and therefore $a \equiv a \mod n$ (by the definition of congruence).

(b) Let $a, b \in \mathbb{Z}$ satisfy $a \equiv b \mod n$. We must prove $b \equiv a \mod n$.

From $a \equiv b \mod n$, we obtain $n \mid a - b \mid (a - b)(-1) = b - a$. Hence, $b \equiv a \mod n$.

(c) Let $a, b, c \in \mathbb{Z}$ satisfy $a \equiv b \mod n$ and $b \equiv c \mod n$. We must prove that $a \equiv c \mod n$.

From $a \equiv b \mod n$, we obtain $n \mid a - b$.

From $b \equiv c \mod n$, we obtain $n \mid b - c$.

So we know that both $a - b$ and $b - c$ are multiples of n. Hence, their sum $(a - b) + (b - c)$ is also a multiple of n. Since this sum is just $a - c$, this means that $a - c$ is a multiple of n. In other words, $a \equiv c \mod n$.

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

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

From $a_1 \equiv b_1 \mod n$, we see that $n \mid a_1 - b_1$. In other words, $a_1 - b_1 = nc_1$ for some $c_1 \in \mathbb{Z}$. Consider this c_1. Solving this equation for a_1, we find $a_1 = b_1 + nc_1$.

Similarly, $a_2 = b_2 + nc_2$ for some $c_2 \in \mathbb{Z}$. Consider this c_2.

Now,

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

so that $(a_1 + a_2) - (b_1 + b_2) = n(c_1 + c_2)$ is a multiple of n. This shows that $a_1 + a_2 \equiv b_1 + b_2 \mod n$.

A similar argument shows that $a_1 - a_2 \equiv b_1 - b_2 \mod n$.

Furthermore,

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

so that $a_1 a_2 - b_1 b_2 = n(b_1 c_2 + c_1 b_2 + nc_1 c_2)$ is a multiple of n. This shows that $a_1 a_2 \equiv b_1 b_2 \mod n$.

(e) Assume that $a, b \in \mathbb{Z}$ satisfy $a \equiv b \mod n$. Thus, $n \mid a - b$, therefore $m \mid n \mid a - b$. Hence, $m \mid a - b$, so that $a \equiv b \mod m$. □

Part **(b)** of the above proposition tells us that congruences can be turned around ($a \equiv b \mod n$ implies $b \equiv a \mod n$).

Part **(c)** says that congruences can be chained together ($a \equiv b \mod n$ and $b \equiv c \mod n$ imply $a \equiv c \mod n$). You will often see the notation "$a \equiv b \equiv c \mod n$" for "$a \equiv b \mod n$ and $b \equiv c \mod n$". More generally, the statement

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

means that each of the numbers $a_1, a_2, \ldots, a_k$ is congruent to the next modulo n. By induction on k, this can easily be shown to imply $a_1 \equiv a_k \mod n$ and actually $a_i \equiv a_j \mod n$.

Note that we cannot chain two congruences together if they have different n's. For example, from $a \equiv b \mod 2$ and $b \equiv c \mod 3$, you cannot conclude any congruence between a and c.

Part **(d)** of the proposition gives us the right to add, subtract and multiply two congruences modulo the same n. Note that you cannot divide two such congruences, or take one to the other's power. That is, from

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

you **cannot** conclude that $\dfrac{a_1}{a_2} \equiv \dfrac{b_1}{b_2} \mod n$ or that $a_1^{a_2} \equiv b_1^{b_2} \mod n$ (even when all the numbers in question are integers). However, we can at least take a congruence to a fixed power:

> **Exercise 3.2.1.** Let $n, a, b \in \mathbb{Z}$ be such that $a \equiv b \mod n$. Then, $a^k \equiv b^k \mod n$ for any $k \in \mathbb{N}$.

3.2.3. Proving the divisibility criteria

Recall the criterion for divisibility by 9:

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

Proof. Let $m_d m_{d-1} \cdots m_0$ be the decimal representation of m. 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, $10 \equiv 1 \mod 9$ (since $10 - 1 = 9$ is a multiple of 9). Hence, by the exercise we just showed, $10^k \equiv 1^k \mod 9$ for every $k \in \mathbb{N}$. Multiplying this congruence by the obvious congruence $m_k \equiv m_k \mod 9$, we obtain

$$m_k \cdot 10^k \equiv m_k \cdot 1^k \mod 9 \qquad \text{for each } k \in \{0, 1, \ldots, d\}.$$

In other words,

$$m_k \cdot 10^k \equiv m_k \mod 9 \qquad \text{for each } k \in \{0, 1, \ldots, d\}.$$

These are $d + 1$ congruences. Adding them together, we get

$$\begin{aligned} &m_d \cdot 10^d + m_{d-1} \cdot 10^{d-1} + \cdots + m_0 \cdot 10^0 \\ &\equiv m_d + m_{d-1} + \cdots + m_0 \mod 9. \end{aligned}$$

In other words,

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

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

Now, if $9 \mid m$, then $m \equiv 0 \bmod 9$, so that $s \equiv m \equiv 0 \bmod 9$, thus $s \equiv 0 \bmod 9$, meaning that $9 \mid s$.

Conversely, a similar argument shows that $9 \mid s$ implies $9 \mid m$.

Thus, $9 \mid m$ is equivalent to $9 \mid s$. This proves the proposition. □

The same argument works for divisibility by 3, because $10 \equiv 1 \bmod 3$.

3.3. Division with remainder

3.3.1. The theorem

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. First, some notations:

Definition 3.3.2. Let n be an integer. Let d be a positive integer. Let (q, r) be the pair whose existence and uniqueness is claimed in the above theorem. Then:

- The number q is called the **quotient** of the division of n by d, and is denoted by $n//d$. (In LaTeX: // and \sslash.)
- The number r is called the **remainder** of the division of n by d, and is denoted by $n\%d$. (In LaTeX: \%.)
- The pair (q, r) is called the **quo-rem pair** of n and d.

As we have not yet proved that these q and r exist and are unique, we shall use indefinite articles ("a quotient", "a remainder", "a quo-rem pair") until we have finished that proof.

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

$$8//5 = 1 \qquad \text{and} \qquad 8\%5 = 3,$$

since

$$\underbrace{8}_{=n} = \underbrace{1}_{=q} \cdot \underbrace{5}_{=d} + \underbrace{3}_{=r\in\{0,1,2,3,4\}} .$$

Example 3.3.4. What are 29//3 and 29%3 ? We have

$$29//3 = 9 \qquad \text{and} \qquad 29\%3 = 2,$$

since

$$29 = 9 \cdot 3 + 2.$$

Example 3.3.5. What are $(-7)\,//5$ and $(-7)\,\%5$? We have $(-7)\,//5 = -2$ and $(-7)\,\%5 = 3$, since

$$-7 = (-2) \cdot 5 + \underbrace{3}_{\in\{0,1,2,3,4\}} .$$

Our theorem is saying that any integer n and any positive integer d have a unique quo-rem pair. Let us now prove this.

3.3.2. The proof

Proof. We need to prove two things: that a quo-rem pair of n and d exists, and that it is unique. Let us start with the uniqueness part.

Proof of the uniqueness part: Fix an integer n and a positive integer d. We must show that there is **at most one** quo-rem pair (q, r) of n and d.

Assume the contrary. Thus, there exist two distinct quo-rem pairs (q_1, r_1) and (q_2, r_2) of n and d. Pick two such pairs.

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

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

Since (q_2, r_2) is a quo-rem pair of n and d, we have

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

Subtracting the equations $n = q_1 d + r_1$ and $n = q_2 d + r_2$, we obtain

$$0 = (q_1 d + r_1) - (q_2 d + r_2) = (r_1 - r_2) + (q_1 - q_2)\, d.$$

Thus,

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

We are in one of the following three cases:

Case 1: We have $q_1 < q_2$.

Case 2: We have $q_1 = q_2$.

Case 3: We have $q_1 > q_2$.

Consider Case 1. In this case, $q_1 < q_2$, so that $q_2 - q_1 > 0$. Hence, $q_2 - q_1 \geq 1$. Since $d > 0$, this entails $(q_2 - q_1) d \geq 1d = d$. Thus,

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

However, this contradicts

$$r_1 - \underbrace{r_2}_{\geq 0} \leq r_1 \leq d - 1 < d.$$

Thus, we have found a contradiction in Case 1.

Consider Case 2. In this case, $q_1 = q_2$. Hence, $\underbrace{(q_2 - q_1)}_{=0} d = 0$. Thus,

$$r_1 - r_2 = (q_2 - q_1) d = 0,$$

so that $r_1 = r_2$. Combining this with $q_1 = q_2$, we obtain $(q_1, r_1) = (q_2, r_2)$. This contradicts the assumption that (q_1, r_1) and (q_2, r_2) are distinct. So we found a contradiction in Case 2 as well.

Consider Case 3. In this case, $q_1 > q_2$, so that $q_2 < q_1$. Thus Case 3 is just Case 1 with the roles of (q_1, r_1) and (q_2, r_2) switched. Thus, we again get a contradiction.

We have now found a contradiction in each case. So our assumption was wrong. This proves the uniqueness of a quo-rem pair.

Now, let us come to the existence part. We want to argue by strong induction on n, but this only covers the case $n \geq 0$. The case $n < 0$ will have to be handled separately afterwards.

So let us first deal with the $n \geq 0$ case:

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

Proof of the lemma. Fix d. We use strong induction on n (without a base case).

Induction step: Let $n \in \mathbb{N}$. Assume (as the IH) that the lemma holds for all nonnegative integers smaller than n instead of n. In other words, assume that for each nonnegative integer $k < n$, there exists a quo-rem pair of k and d. We must prove that the lemma also holds for n, i.e., that there exists a quo-rem pair of n and d.

If $n < d$, then such a pair is easy to find: it is $(0, n)$ (since $n = 0d + n$ and $n \in \{0, 1, \ldots, d-1\}$).

Otherwise, $n \geq d$, so that $n - d \in \mathbb{N}$ and $n - d < n$ (since $d > 0$). This means that we can apply the IH to $n - d$ instead of n. This yields that there exists a quo-rem pair of $n - d$ and d. Let (q, r) be this pair. Then,

$$n - d = qd + r.$$

Hence,

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

This shows that $(q+1, r)$ is a quo-rem pair of n and d. Thus, we have found a quo-rem pair of n and d, as we desired. This completes the induction step, and thus the lemma is proved. □

So we have proved that

- there is **always at most one** quo-rem pair of n and d;
- there is **at least one** such pair if $n \geq 0$.

It remains to prove that there is **at least one** such pair if $n < 0$.

One way to do this is by a strong induction (similarly to the lemma), but now inducting on $-n$, not on n.

A slicker way is by reducing the $n < 0$ case to the $n \geq 0$ case: Namely, let $n \in \mathbb{Z}$ be negative. Then, the product $\underbrace{(1-d)}_{\leq 0} \underbrace{n}_{<0}$ is nonnegative. Hence, by our lemma, there exists a quo-rem pair for $(1-d)\, n$ and d. Let (q, r) be this pair. Then,

$$\begin{aligned} (1-d)\, n &= qd + r, && \text{that is,} \\ n - nd &= qd + r, && \text{that is,} \\ n &= nd + qd + r = (n+q)\, d + r. \end{aligned}$$

This shows that $(n+q, r)$ is a quo-rem pair for n and d. So n and d have a quo-rem pair. This completes the proof. □

3.3.3. Application: even and odd integers

Recall that an integer n is **even** if $2 \mid n$, and is **odd** if $2 \nmid n$. This is how we defined "even" and "odd". Let us now prove a different criterion:

Proposition 3.3.7. Let n be an integer.

(a) The integer n is even if and only if there exists some $k \in \mathbb{Z}$ such that $n = 2k$.

(b) The integer n is odd if and only if there exists some $k \in \mathbb{Z}$ such that $n = 2k+1$.

Proof. **(a)** follows from the definitions.

(b) This is an "if and only if" statement, so we need to prove both directions:

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

and

$$(n \text{ is odd}) \Longleftarrow (\text{there exists some } k \in \mathbb{Z} \text{ such that } n = 2k+1)\,.$$

Proof of the $\Longrightarrow$ direction: Assume that n is odd. By the theorem we just proved, there exists a quo-rem pair (q,r) for n and 2. This pair satisfies

$$q \in \mathbb{Z}, \qquad r \in \{0,1\}, \qquad \text{and} \qquad n = 2q + r.$$

If we had $r = 0$, then this would yield $n = 2q + \underbrace{r}_{=0} = 2q$, contradicting the oddness of n. So $r \neq 0$. Therefore, $r = 1$ (since $r \in \{0,1\}$). Thus, $n = 2q + \underbrace{r}_{=1} = 2q + 1$. This shows that there exists some $k \in \mathbb{Z}$ such that $n = 2k+1$ (namely, $k = q$).

Proof of the $\Longleftarrow$ direction: Assume that there exists some $k \in \mathbb{Z}$ such that $n = 2k+1$. Consider this k.

We must prove that n is odd. In other words, we must prove that $2 \nmid n$. Assume the contrary. Thus, $2 \mid n$. In other words, $n = 2c$ for some integer c. Consider this c.

Now, $(k,1)$ is a quo-rem pair of n and 2 (since $n = 2k+1$ and $1 \in \{0,1\}$), but $(c,0)$ is also a quo-rem pair of n and 2 (since $n = 2c = 2c + 0$ and $0 \in \{0,1\}$). So n and 2 have (at least) two distinct quo-rem pairs, which is impossible by the uniqueness part of the preceding theorem. So we get a contradiction, exactly as desired. □

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

Proof. **(c)** Two odd integers can be written as $2k+1$ and $2\ell+1$ for some integers k and ℓ (by the preceding proposition). Hence, their sum is

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

which is clearly even.

(a), **(b)** are similar. □

Note that part **(c)** of this corollary would not hold for other divisors than 2. For instance, a sum of two integers that are not divisible by 3 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. We set $q := n//d$ and $r := n\%d$. Thus, (q, r) is a quo-rem pair of n and d. In other words, $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, d-1\}$ and $n = qd + r$.

(d) We have $n = \underbrace{q}_{=n//d} d + \underbrace{r}_{=n\%d} = (n//d)\, d + (n\%d)$.

(a) We have $n\%d = r \in \{0, 1, \ldots, d-1\}$. Next, $n = qd + r$ entails $n - r = qd$, which is a multiple of d. Hence, $n \equiv r \bmod d$. Thus, $r \equiv n \bmod d$. In other words, $n\%d \equiv n \bmod d$ (since $n\%d = r$).

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

The congruence $c \equiv n \bmod d$ entails $n \equiv c \bmod d$, so that $d \mid n - c$. In other words, $n - c = dx$ for some integer x. Consider this x.

Now, $n - c = dx$ entails $n = dx + c = xd + c$, and this shows that (x, c) is a quo-rem pair of n and d (since $c \in \{0, 1, \ldots, d-1\}$). Hence, $c = n\%d$ (here we are tacitly using the uniqueness of the quo-rem pair).

(b) This is an "if and only if" statement, so we should prove both directions.

$\Longrightarrow$: Assume that $d \mid n$. We must prove that $n\%d = 0$.

From $d \mid n$, we see that $n = dx$ for some integer x. Thus, $n = dx + 0$, so that $(x, 0)$ is a quo-rem pair of n and d. Hence, $0 = n\%d$.

Alternatively: From $d \mid n$, we see that $n \equiv 0 \bmod d$. So $0 \equiv n \bmod d$. Since $0 \in \{0, 1, \ldots, d-1\}$, we can thus apply part **(c)** to $c = 0$, and obtain that $0 = n\%d$. Hence, $n\%d = 0$.

$\Longleftarrow$: Assume that $n\%d = 0$. We must prove that $d \mid n$.

We have $n = qd + \underbrace{r}_{=n\%d=0} = qd$, so that $d \mid n$.

(e) Either induct on n (as in the proof of the lemma), or "chase inequalities" (use the fact that any integer that is > -1 is automatically ≥ 0). For details, see the notes (Proposition 3.3.11 **(e)**). □

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 $n\%2 = 1$.

Quotients and remainders are closely related to the floor function:

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

For example,

$$\lfloor 3.8 \rfloor = 3, \qquad \lfloor \pi \rfloor = 3, \qquad \lfloor 3 \rfloor = 3, \qquad \lfloor -\pi \rfloor = -4.$$

Proposition 3.3.12 ("explicit formulas" for quotient and remainder)**.** Let $n \in \mathbb{Z}$, and let d be a positive integer. Then,

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

Proof. The main idea is the following: Two numbers u and x satisfy $u = \lfloor x \rfloor$ if and only if u is an integer and $u \leq x < u + 1$.

Thus you can prove $n//d = \left\lfloor \dfrac{n}{d} \right\rfloor$ by showing that $n//d \leq \dfrac{n}{d} < (n//d) + 1$. The latter is fairly easy (see the notes).

Having proved this, the other equality $n\%d = n - d \cdot \left\lfloor \dfrac{n}{d} \right\rfloor$ follows easily using $n = (n//d)\, d + (n\%d)$. □

3.3.5. Base-b representation of nonnegative integers

Division with remainder is the main ingredient in a useful feature of integers: the fact that every integer can be uniquely expressed in decimal notation, or, more general, in base-b notation for any given integer $b > 1$.

What does this mean for $b = 10$? For instance,

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

Thus, the big number 3401 has been written as a sum of powers of 10, with the coefficients $3, 4, 0, 1$ being integers between 0 and 9 (commonly called "digits").

This can be done for any $n \in \mathbb{N}$ instead of 3401, and for any fixed integer $b > 1$ instead of 10. The coefficients will then be integers between 0 and $b - 1$. This is called the "base-b representation" of the integer.

For instance, let us find the base-4 representation of 3401: This will be a representation of the form

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

where each r_i is a "base-4 digit" (i.e., an element of $\{0, 1, 2, 3\}$). At least, this is how it will look like if 7 digits are enough. If not, we need $r_7, r_8, \ldots$, whatever amount will suffice.

How do we find these base-4 digits $r_0, r_1, \ldots, r_6$?

We start by looking at the equation

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

Thus,

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

So we have found r_0. Now,

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

Thus,

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

So we have found r_1.

Keep doing this to find r_2, r_3, r_4, r_5, r_6 in succession. We get

$$r_2 = 0, \qquad r_3 = 1, \qquad r_4 = 1, \qquad r_5 = 3, \qquad r_6 = 0.$$

So the base-4 representation of 3401 is

$$3401 = \underbrace{r_6}_{=0} 4^6 + \underbrace{r_5}_{=3} 4^5 + \underbrace{r_4}_{=1} 4^4 + \underbrace{r_3}_{=1} 4^3 + \underbrace{r_2}_{=0} 4^2 + \underbrace{r_1}_{=2} 4^1 + \underbrace{r_0}_{=1} 4^0.$$

One typically states this as "the number 3401 written in base-4 is 0311021". Commonly, one omits leading 0's, so this would just be 311021.

This method works for any integer $b > 1$ instead of 4, and any $n \in \mathbb{N}$ instead of 3401. The idea is to divide n by b with remainder; then divide the quotient again by b with remainder; then divide the resulting quotient again by b with remainder; and so on. The remainders obtained will be the base-b digits of n (from right to left). The following theorem makes this formal:

Theorem 3.3.13. Let $b > 1$ be an integer. Let $n \in \mathbb{N}$. Then:

(a) We can write n in the form

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

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

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

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, they can be explicitly computed by the formula

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

Proof. See the notes (Theorem 3.3.15). □

3.3.6. Congruence in terms of remainders

The next proposition formalizes the close relation between remainders and congruence:

> **Proposition 3.3.14.** Let d be a positive integer. Let a and b be two integers. Then, $a \equiv b \bmod d$ if and only if $a\%d = b\%d$.

Proof. We must prove the logical equivalence

$$(a \equiv b \bmod d) \Longleftrightarrow (a\%d = b\%d).$$

Let us prove its $\Longrightarrow$ and $\Longleftarrow$ directions separately:

$\Longrightarrow$: Assume that $a \equiv b \bmod d$. We must prove that $a\%d = b\%d$.

Recall that $a\%d \in \{0, 1, \ldots, d-1\}$ and $a\%d \equiv a \bmod d$. Hence,

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

Thus, $a\%d \equiv b \bmod d$. So $a\%d$ is an integer in the set $\{0, 1, \ldots, d-1\}$ that is congruent to b modulo d. But the only such integer is $b\%d$. So we get $a\%d = b\%d$.

$\Longleftarrow$: Assume that $a\%d = b\%d$. We must prove that $a \equiv b \bmod d$.

Again recall that $a\%d \equiv a \bmod d$. Similarly, $b\%d \equiv b \bmod d$. Hence,

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

So $a \equiv b \bmod d$. □

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

3.3.7. The birthday lemma

Assume, for simplicity, that any year has 365 days (so no leapyears). If you have lived for exactly n days, then you are $n//365$ years and $n\%365$ days old. 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 former number ($n//365$) increases by 1 whereas the latter number ($n\%365$) gets reset to 0.

This has nothing to do with 365; it holds for any positive integer d and any $n \in \mathbb{Z}$:

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

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

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

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

Proof. See the notes. □

The equalities for $n//d$ in the above proposition can also be stated in terms of the floor function:

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

3.4. Greatest common divisors

3.4.1. Definition

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 the case $a = b = 0$, we define it to be 0 instead.

We denote the greatest common divisor of a and b by $\gcd(a, b)$, and we 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 therefore $-2, -1, 1, 2$. The largest among them is 2.

  So $\gcd(4, 6) = 2$.

- 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 therefore exactly the divisors of 5, and the largest of them is 5.

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

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

  It is 0 by definition. (The common divisors of 0 and 0 are all the integers, so there is no largest among them.)

Proposition 3.4.2. Let $a, b \in \mathbb{Z}$. Then, $\gcd(a,b)$ is well-defined.

Proof. If $a = b = 0$, then $\gcd(a,b) = 0$ by definition.

Let us consider the remaining case, i.e., the case when a and b are not both 0. In this case, we defined $\gcd(a,b)$ to be the largest among the common divisors of a and b. To check that it is well-defined, we shall show that the set of common divisors of a and b is finite and nonempty (because then, it follows that this set has a unique largest element, i.e., there is a largest common divisor of a and b).

- **Finiteness:** If $a \neq 0$, then any divisor of a has absolute value $\leq |a|$, which leaves only finitely many choices for the divisor. If $b \neq 0$, then a similar argument applies. Since a and b are not both 0, this covers all possibilities.

- **Nonemptiness:** There is at least one common divisor of a and b, because the number 1 is such a common divisor.

□

3.4.2. Basic properties

Our goal is to find an easier way to compute $\gcd(a,b)$ than by checking all divisors of a and/or of b.

Proposition 3.4.3. We have $\gcd(a,b) \in \mathbb{N}$ for any $a, b \in \mathbb{Z}$.

Proof. If $a = b = 0$, then this is clear since $\gcd(0,0) = 0 \in \mathbb{N}$.

In the remaining case, $\gcd(a,b)$ is literally the largest of the common divisors of a and b. However, if it was negative, then $-\gcd(a,b)$ would be an even larger common divisor of a and b, which would contradict this. So $\gcd(a,b)$ cannot be negative. Thus, $\gcd(a,b) \in \mathbb{N}$. □

Proposition 3.4.4. We have $\gcd(a,0) = \gcd(0,a) = |a|$ for any $a \in \mathbb{Z}$.

Proof. Let $a \in \mathbb{Z}$. All integers are divisors of 0. So the common divisors of a and 0 are precisely the divisors of a. The largest of those is $|a|$ (unless $a = 0$, but this case is obvious anyway). □

Proposition 3.4.5. We have $\gcd(a,b) = \gcd(b,a)$ for any $a, b \in \mathbb{Z}$.

Proof. The definition is symmetric in a and b. □

Proposition 3.4.6. If $a, b, c \in \mathbb{Z}$ satisfy $b \equiv c \bmod a$, then $\gcd(a,b) = \gcd(a,c)$.

Proof. Let $a, b, c \in \mathbb{Z}$ satisfy $b \equiv c \bmod a$. We must prove $\gcd(a,b) = \gcd(a,c)$.

If $a = 0$, then this is clear (since $b \equiv c \bmod a$ yields $b = c$)

So we only need to deal with the case $a \neq 0$. Consider this case. Here, $\gcd(a,b)$ is literally the greatest common divisor of a and b, whereas $\gcd(a,c)$ is literally the greatest common divisor of a and c. We must prove that they are equal. We shall prove even more: We shall show that the common divisors of a and b are precisely the common divisors of a and c.

To show this, we must prove the following two claims:

> *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.

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.

The definition of d yields $d \mid a$ and $d \mid b$. It remains to show that $d \mid c$ as well.

From $b \equiv c \bmod a$, we obtain $a \mid b - c$, so that $d \mid a \mid b - c$. In other words, $b - c = dz$ for some integer z. Also, $b = dy$ for some integer y (since $d \mid b$). Using these z and y, we have

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

This shows that $d \mid c$. So Claim 1 is proved. □

Proof of Claim 2. The numbers b and c are playing equal roles in our setting (since $b \equiv c \bmod a$ entails $c \equiv b \bmod a$). So Claim 2 is just Claim 1, with the roles of b and c interchanged. □

Both claims are now proved. It follows that the common divisors of a and b are the common divisors of a and c. Hence, the greatest of the former is the greatest of the latter. In other words, $\gcd(a,b) = \gcd(a,c)$. □

Proposition 3.4.7. We have $\gcd(a,b) = \gcd(a,\ ua+b)$ for any $a,b,u \in \mathbb{Z}$.

Proof. Let $a,b,u \in \mathbb{Z}$. Then, $b \equiv ua + b \bmod a$. Thus, the preceding proposition (applied to $c = ua+b$) yields $\gcd(a,b) = \gcd(a,\ ua+b)$. □

Proposition 3.4.8. Let a be a positive integer. Let $b \in \mathbb{Z}$. Then, $\gcd(a,b) = \gcd(a,\ b\%a)$.

Proof. We have $b \equiv b\%a \bmod a$ (by one of the basic properties of quotients and remainders). Hence, the second-to-previous proposition (applied to $c = b\%a$) yields $\gcd(a,b) = \gcd(a,\ b\%a)$. □

The following facts are very easy:

Proposition 3.4.9. We have $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$ for any $a,b \in \mathbb{Z}$.

Proposition 3.4.10. We have $\gcd(-a,b) = \gcd(a,b)$ and $\gcd(a,-b) = \gcd(a,b)$ for any $a,b \in \mathbb{Z}$.

Proposition 3.4.11. If $a,b \in \mathbb{Z}$ satisfy $a \mid b$, then $\gcd(a,b) = |a|$.

Proof. Let $a,b \in \mathbb{Z}$ satisfy $a \mid b$. Then, $|a|$ is a common divisor of a and b (since it divides a, which in turn divides b). It is furthermore the greatest of these, since any divisor of a is $\leq |a|$. (Again, this does not work for $a = 0$, but this case is trivial.) □

Corollary 3.4.12 (Euclidean recursion for the gcd)**.** Let $a \in \mathbb{Z}$, and let b be a positive integer. Then,

$$\gcd(a,b) = \gcd(b,\ a\%b).$$

Proof. We have

$$\gcd(a,b) = \gcd(b,a) = \gcd(b,\ a\%b)$$

(by the proposition saying $\gcd(a,b) = \gcd(a,\ b\%a)$, applied to b and a instead of a and b). □

3.4.3. The Euclidean algorithm

By applying the last corollary repeatedly, we can compute gcds fairly quickly. For instance,

$$\begin{aligned}
\gcd(96,\ 18) &= \gcd(18,\ 96\%18) && \text{(by the corollary)} \\
&= \gcd(18,\ 6) \\
&= \gcd(6,\ 18\%6) && \text{(by the corollary)} \\
&= \gcd(6,\ 0) \\
&= |6| && \text{(by the proposition } \gcd(a,0) = |a|\text{)} \\
&= 6
\end{aligned}$$

and

$$\begin{aligned}
\gcd(1135,\ 739) &= \gcd(739,\ 1135\%739) && \text{(by the corollary)} \\
&= \gcd(739,\ 396) \\
&= \gcd(396,\ 739\%396) && \text{(by the corollary)} \\
&= \gcd(396,\ 343) \\
&= \gcd(343,\ 396\%343) && \text{(by the corollary)} \\
&= \gcd(343,\ 53) \\
&= \gcd(53,\ 343\%53) && \text{(by the corollary)} \\
&= \gcd(53,\ 25) \\
&= \gcd(25,\ 53\%25) && \text{(by the corollary)} \\
&= \gcd(25,\ 3) \\
&= \gcd(3,\ 25\%3) && \text{(by the corollary)} \\
&= \gcd(3,\ 1) \\
&= \gcd(1,\ 3\%1) && \text{(by the corollary)} \\
&= \gcd(1,0) \\
&= |1| && \text{(by the } \gcd(a,0) = |a| \text{ proposition)} \\
&= 1.
\end{aligned}$$

These two computations are instances of a general algorithm for computing $\gcd(a,b)$ for any two numbers $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. This algorithm proceeds as follows:

- If $b = 0$, then the gcd is $|a|$.
- If $b > 0$, then we replace a and b by b and $a\%b$ and recurse (i.e., we apply the method again to b and $a\%b$ instead of a and b).

In Python code, this algorithm looks as follows:

```
def gcd(a, b):  # for b nonnegative
    if b == 0:
        return abs(a) # this means |a|
    return gcd(b, a%b)
```

This algorithm is known as the **Euclidean algorithm**. Let us convince ourselves that this algorithm terminates (i.e., does not get stuck in an infinite loop):

Proposition 3.4.13. Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then, the Euclidean algorithm terminates after at most b steps.

Proof. (See the notes for details.)

Every time the algorithm recurses (i.e., replaces a and b by b and $a\%b$ and calls itself again), the value of b decreases by at least 1 (since $a\%b \leq b - 1$).

But a nonnegative integer cannot keep decreasing by at least 1 infinitely often. More concretely, decreasing b by at least 1 can be done at most b times until b becomes negative. □

Actually, the "b steps" in the proposition greatly overestimate the time that the Euclidean algorithm needs to terminate. A much better bound is $\log_2(ab) + 2$ steps (assuming that $a, b > 0$). See the notes for why this better bound holds.

The Euclidean algorithm can be easily adapted to arbitrary $b \in \mathbb{Z}$ instead of just $b \in \mathbb{N}$:

```
def gcd(a, b):  # for b arbitrary
    if b < 0:
        return gcd(a, -b)
    if b == 0:
        return abs(a) # this means |a|
    return gcd(b, a%b)
```

3.4.4. Bezout's theorem and the extended Euclidean algorithm

The Euclidean algorithm can be adapted to not only compute $\gcd(a,b)$, but also represent $\gcd(a,b)$ as an "integer linear combination" of a and b (i.e., as a multiple of a plus a multiple of b). This lets us prove the following theorem:

Theorem 3.4.14 (Bezout's theorem for integers)**.** Let a and b be two integers. Then, there exist two integers x and y such that

$$\gcd(a,b) = xa + yb.$$

This can be restated as a claim about a coin problem: It says that $\gcd(a,b)$ cents can be paid with a-cent and b-cent coins, as long as you can get change.

Before we prove this theorem, let me give these x and y a name:

Definition 3.4.15. Let a and b be two integers. Then, a **Bezout pair** for (a,b) means a pair (x,y) of two integers such that $\gcd(a,b) = xa + yb$.

For instance:

- A Bezout pair for $(4,7)$ is a pair (x,y) of two integers such that $\gcd(4,7) = x \cdot 4 + y \cdot 7$, that is, $1 = x \cdot 4 + y \cdot 7$. One such pair is $(2,-1)$, since $1 = 2 \cdot 4 + (-1) \cdot 7$. There are other such pairs as well, for instance $(-5,3)$.

- A Bezout pair for $(4,6)$ is a pair (x,y) of two integers such that $\gcd(4,6) = x \cdot 4 + y \cdot 6$, that is, $2 = x \cdot 4 + y \cdot 6$. One such pair is $(-1,1)$.

How would you prove Bezout's theorem? Induction sounds like a good idea, but induction needs to start somewhere, whereas both a and b in the theorem are just integers.

Fortunately, we can adapt to this. Indeed, if we can prove Bezout's theorem for $b \in \mathbb{N}$, then it easily follows for all $b \in \mathbb{Z}$, because if (u, v) is a Bezout pair for (a, b), then $(u, -v)$ is a Bezout pair for $(a, -b)$ (since $\gcd(a, b) = \gcd(a, -b)$ and $ua + (-v)(-b) = ua + vb$). So it suffices to prove Bezout's theorem for $b \in \mathbb{N}$. In other words, it suffices to prove the following:

Lemma 3.4.16. Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then, there exists a Bezout pair for (a, b).

Proof. Strong induction on b. In more detail: We do not fix a. We consider the statement

$$P(b) := (\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a, b)).$$

We want to prove this statement $P(b)$ for all $b \in \mathbb{N}$. We do this by strong induction on b:

Base case: We must prove $P(0)$. This is easy: A Bezout pair for $(a, 0)$ is $(\pm 1, 0)$, where ± 1 is $+1$ or -1 depending on whether $a \geq 0$ or $a < 0$.

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 that $P(0)$ AND $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(b-1)$ holds. In other words, we assume that

$$\begin{aligned}
&(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a, 0)) \text{ and}\\
&(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a, 1)) \text{ and}\\
&(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a, 2)) \text{ and}\\
&\cdots \text{ and}\\
&(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a, b-1))
\end{aligned}$$

hold. 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). So this is our IH.

We must prove that $P(b)$ holds. In other words, we must prove that for each $a \in \mathbb{Z}$, there exists a Bezout pair for (a, b).

Let us do this. Fix $a \in \mathbb{Z}$. Since $b > 0$, we can divide a by b with remainder. We know that $a\%b \in \{0, 1, \ldots, b-1\}$. So we can apply our IH to b and $a\%b$ instead of a and b. We conclude that there exists a Bezout pair for $(b,\ a\%b)$. This is a pair (u, v) of integers such that

$$\gcd(b,\ a\%b) = ub + v(a\%b).$$

Consider this pair. The Euclidean recursion yields

$$\begin{aligned}\gcd(a,b) &= \gcd(b,\ a\%b) = ub + v \underbrace{(a\%b)}_{\substack{=a-(a//b)b \\ (\text{since } a=(a//b)b+(a\%b))}} \\ &= ub + v\left(a - (a//b)\,b\right) \\ &= va + \left(u - v\,(a//b)\right) b.\end{aligned}$$

This shows that the pair $(v,\ u - v\,(a//b))$ is a Bezout pair for (a,b). So we have shown that there exists a Bezout pair for (a,b). This completes the induction step, and therefore the proof of the lemma. □

And, as we explained, the lemma yields Bezout's theorem. In Python, this algorithm looks as follows:

```
def bezout_pair(a, b):  # for b nonnegative
    if b == 0:
        return (sign(a), 0)
    (u, v) = bezout_pair(b, a%b)
    return (v, u - v * (a//b))
```

This algorithm is known as the **extended Euclidean algorithm**. As explained, we can easily adapt it to negative b. (See the notes for details.)

3.4.5. The universal property of the gcd

The first major application of the extended Euclidean algorithm is the **universal property of the gcd**:

> **Theorem 3.4.17** (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 $\gcd(a,b)$. So $\gcd(a,b)$ is not just the greatest of all common divisors of a and b, but also a multiple of each of them.

Proof of the universal property. $\Longleftarrow$: If $m \mid \gcd(a,b)$, then $m \mid a$ (since $m \mid \gcd(a,b) \mid a$) and $m \mid b$ (similarly).

$\Longrightarrow$: Assume that $m \mid a$ and $m \mid b$. We must prove that $m \mid \gcd(a,b)$.

Bezout's theorem yields that $\gcd(a,b) = xa + yb$ for some integers x and y. Consider these x and y.

From $m \mid a$, we know that a is a multiple of m. Thus, xa is also a multiple of m. Similarly, yb is a multiple of m. Hence, the sum $xa + yb$ is a multiple of m as well (since a sum of multiples of m is again a multiple of m). In other words, $\gcd(a,b)$ is a multiple of m (since $\gcd(a,b) = xa + yb$). In other words, $m \mid \gcd(a,b)$. □

3.4.6. Factoring out a common factor from a gcd

The following theorem may sound obvious, but actually is not. We shall prove it using the universal property:

> **Theorem 3.4.18.** Let $s, a, b \in \mathbb{Z}$. Then,
>
> $$\gcd(sa, sb) = |s| \cdot \gcd(a, b).$$

Proof. Let

$$g = \gcd(a, b) \qquad \text{and} \qquad h = \gcd(sa, sb).$$

We must prove that $h = |s| \cdot g$. Equivalently, we must prove that $|h| = |sg|$ (since g and h are nonnegative, so that $|g| = g$ and $|h| = h$, and $|sg| = |s| \cdot |g| = |s| \cdot g$).

One good way to prove that two integers p and q satisfy $|p| = |q|$ (i.e., are equal up to sign) is by showing that $p \mid q$ and $q \mid p$. So, in order to prove that $|h| = |sg|$, we only need to show that $h \mid sg$ and $sg \mid h$. Let us show this:

- *Proof of $sg \mid h$:* We have $g = \gcd(a, b) \mid a$. Thus, $sg \mid sa$. Similarly, $sg \mid sb$. Hence, the universal property of the gcd yields $sg \mid \gcd(sa, sb)$. In other words, $sg \mid h$ (since $h = \gcd(sa, sb)$).

- *Proof of $h \mid sg$:* We have $h = \gcd(sa, sb) \mid sa$. In other words, $sa = hu$ for some integer u. Similarly, $sb = hv$ for some integer v. Consider these u and v.

  However, Bezout's theorem shows that $\gcd(a, b) = xa + yb$ for some integers x and y. Consider these x and y.

  Now, $g = \gcd(a, b) = xa + yb$. Hence,

  $$\begin{aligned} sg &= s(xa + yb) = sxa + syb = \underbrace{sa}_{=hu} x + \underbrace{sb}_{=hv} y \\ &= hux + hvy = h \underbrace{(ux + vy)}_{\text{an integer}}, \end{aligned}$$

  so that $h \mid sg$.

  (See the notes – proof of Theorem 3.4.11 – for a different way of showing this.)

□

3.5. Coprime integers

3.5.1. Definition and examples

Greatest common divisors are most useful when they equal 1. This situation 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: If a and b are coprime, then b and a are coprime (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, we know that $\gcd(n,2)$ is a divisor of 2 and is a nonnegative integer. But the only nonnegative divisors of 2 are 1 and 2. Hence, $\gcd(n,2)$ must always be 1 or 2. Now:

- If $\gcd(n,2) = 2$, then n is even (since $2 = \gcd(n,2) \mid n$).
- If $\gcd(n,2) = 1$, then n is odd (since otherwise, 2 would be a common divisor of n and 2, but this cannot happen when the greatest common divisor is 1).

(b) An integer n is coprime to 3 if and only if n is not divisible by 3. (This can be shown in the same way, since the only nonnegative divisors of 3 are 1 and 3.)

(c) An integer n is coprime to 4 if and only if n is odd. Indeed, the nonnegative divisors of 4 are 1, 2 and 4, so that $\gcd(n,4)$ is 1, 2 or 4. Now:

- If $\gcd(n,4) = 1$, then n is odd (otherwise, 2 would be a common divisor of n and 4).
- If $\gcd(n,4) = 2$, then n is even (since $2 = \gcd(n,4) \mid n$).
- If $\gcd(n,4) = 4$, then n is even (since $2 \mid 4 = \gcd(n,4) \mid n$).

(d) An integer n is coprime to 5 if and only if n is not divisible by 5. (This is for the same reason as the similar statements about 2 and 3.)

(e) An integer n is coprime to 6 if and only if n is neither even nor divisible by 3. Indeed, the nonnegative divisors of 6 are 1, 2, 3 and 6. Now:

- If $\gcd(n,6) = 1$, then n is not even (since otherwise, 2 would be a common divisor of n and 6) and not divisible by 3 (similarly).
- If $\gcd(n,6) = 2$, then n is even (since $2 = \gcd(n,6) \mid n$).
- If $\gcd(n,6) = 3$, then n is divisible by 3.
- If $\gcd(n,6) = 6$, then n is both even and divisible by 3.

Informally, I tend to think of coprimality as some sort of "unrelatedness" or "independence" or "orthogonality" relation.

3.5.2. Three theorems about coprimality

The following three theorems are useful properties of coprime integers:

> **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, $ab \mid c$.
>
> In other words, a product of two coprime divisors of c is again a divisor of c.

Proof. We have $ab \mid ac$ (since $b \mid c$) and $ba \mid bc$ (since $a \mid c$). Since $ba = ab$ and $ac = ca$ and $bc = cb$, we can rewrite these as follows:

$$ab \mid ca \qquad \text{and} \qquad ab \mid cb.$$

Hence, by the universal property of the gcd, we obtain

$$\begin{aligned} & ab \mid \gcd(ca, cb) \\ & \quad = |c| \cdot \underbrace{\gcd(a,b)}_{\substack{=1 \\ \text{(since } a \text{ and } b \text{ are coprime)}}} \qquad \text{(by the previous theorem)} \\ & \quad = |c| . \end{aligned}$$

Since divisibility is not affected by signs, this entails $ab \mid c$. □

> **Example 3.5.5.** We have $4 \mid 56$ and $7 \mid 56$. Since 4 and 7 are coprime, the coprime divisors theorem thus yields $4 \cdot 7 \mid 56$.
>
> In contrast, from $6 \mid 12$ and $4 \mid 12$, we cannot obtain $6 \cdot 4 \mid 12$, since 6 and 4 are not coprime.

> **Theorem 3.5.6** (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. We have $a \mid ca$ and $a \mid bc = cb$. Thus, by the universal property of the gcd, we get

$$a \mid \gcd(ca, cb) = |c| \cdot \underbrace{\gcd(a,b)}_{\substack{=1 \\ \text{(since } a \text{ and } b \text{ are coprime)}}} = |c| .$$

Since signs do not matter, this entails $a \mid c$. □

Example 3.5.7. We have $6 \mid 7 \cdot 12$, but 6 is coprime to 7. Hence, the coprime removal theorem yields $6 \mid 12$.

Theorem 3.5.8 (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 prove that $g = 1$.

We have $g = \gcd(ab, c) \mid ab$ and $g = \gcd(ab, c) \mid c \mid ac$. Hence, by the universal property of the gcd,

$$g \mid \gcd(ab, ac) = |a| \cdot \underbrace{\gcd(b, c)}_{\substack{=1 \\ \text{(since } b \text{ is coprime to } c\text{)}}} = |a|,$$

so that $g \mid a$. Combining $g \mid a$ and $g \mid c$ using the universal property of the gcd, we obtain $g \mid \gcd(a, c) = 1$ (since a is coprime to c). Thus, $g = 1$ (since the only nonnegative divisor of 1 is 1), as desired. □

See the notes for more general versions of these three theorems.

3.6. Reducing a fraction

One application of the results above is the following:

Theorem 3.6.1. 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.

This theorem is important for understanding rational numbers. Indeed, a **reduced fraction** means a fraction $\frac{u}{v}$ of two integers u and v with $\gcd(u, v) = 1$. The theorem says that if you have any fraction $\frac{a}{b}$ of two integers (not both 0), then you can make it reduced by cancelling $\gcd(a, b)$ from both numerator and denominator.

Proof. Since a and b are not both 0, their gcd is positive. In other words, $g > 0$. Thus, $\frac{a}{g}$ and $\frac{b}{g}$ are well-defined. Moreover, $\frac{a}{g}$ and $\frac{b}{g}$ are integers (since $g = \gcd(a, b) \mid a$ and similarly $g \mid b$).

We have

$$\begin{aligned} g = \gcd(a, b) &= \gcd\left(g\frac{a}{g}, g\frac{b}{g}\right) = |g| \gcd\left(\frac{a}{g}, \frac{b}{g}\right) \\ &= g \gcd\left(\frac{a}{g}, \frac{b}{g}\right) \qquad (\text{since } |g| = g). \end{aligned}$$

Cancelling g (since $g > 0$), we obtain

$$1 = \gcd\left(\frac{a}{g}, \frac{b}{g}\right).$$

In other words, $\frac{a}{g}$ and $\frac{b}{g}$ are coprime, qed. □

3.7. Prime numbers

3.7.1. Definition

Definition 3.7.1. An integer $n > 1$ is said to be **prime** (or **a prime**) if and only 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 (HW) that there are infinitely many primes.

3.7.2. The friend-or-foe lemma

The most fundamental property of primes is what we call the **friend-or-foe lemma**:

Lemma 3.7.2 (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, but not both.

Proof. The number p is prime, so its only positive divisors are 1 and p. Thus, $\gcd(n, p)$ must be 1 or p (since $\gcd(n, p)$ is a positive divisor of p). So we are in one of the following two cases:

Case 1: We have $\gcd(n, p) = 1$.

Case 2: We have $\gcd(n, p) = p$.

Consider Case 1. In this case, $\gcd(n, p) = 1$, so that n is coprime to p. Moreover, n is not divisible by p (since otherwise, p would be a common divisor of n and p, but a common divisor cannot be larger than the gcd, which is 1). So the lemma is proved in Case 1.

Consider Case 2. In this case, $\gcd(n, p) = p > 1$, so that n is not coprime to p. Moreover, n is divisible by p (since $p = \gcd(n, p) \mid n$). So the lemma is proved in Case 2. □

In contrast, if $p > 1$ is not a prime, then there exist integers n that are neither divisible by p nor coprime to p. For instance, 14 is neither divisible by 6 nor coprime to 6.

3.7.3. Binomial coefficients and primes

Pascal's triangle has yet another nice property we have not proved in the previous chapter: If p is prime, then all entries in the p-th row, except for the two 1's at the left and right ends, are divisible by p. In other words:

Theorem 3.7.3. Let p be a prime. Let $k \in \{1, 2, \ldots, p-1\}$. Then, $p \mid \dbinom{p}{k}$.

Proof. Exercise 5 **(a)** on HW#3 yields

$$k \dbinom{p}{k} = p \underbrace{\dbinom{p-1}{k-1}}_{\text{an integer}}.$$

Thus, $p \mid k \dbinom{p}{k}$. If we can show that p is coprime to k, then the coprime removal theorem will thus yield $p \mid \dbinom{p}{k}$, and we will be done. So it remains to show that p is coprime to k.

The friend-or-foe lemma says that k is either divisible by p or coprime to p. Since k cannot be divisible by p (since $k \in \{1, 2, \ldots, p-1\}$), we thus conclude that k is coprime to p. In other words, p is coprime to k. We are done. □

3.7.4. Fermat's little theorem

It is easy to see that every integer a satisfy $a^2 \equiv a \bmod 2$ (since $a^2 - a = a(a-1)$ is divisible by 2, because one of a and $a-1$ is always divisible by 2).

Likewise, every integer a satisfies $a^3 \equiv a \bmod 3$ (since $a^3 - a = (a+1)\,a\,(a-1)$ is divisible by 3).

Unfortunately, the pattern breaks at 4: Not every integer a satisfies $a^4 \equiv a \bmod 4$ (for example, $a = 2$ doesn't).

But the pattern reemerges at 5: Every integer a satisfies $a^5 \equiv a \bmod 5$. (This is a bit harder to check, since $a^5 - a = a(a-1)(a+1)\left(a^2+1\right)$. Nevertheless, it can be checked mechanically, since you can replace a by $a\%5 \in \{0, 1, 2, 3, 4\}$.)

The pattern again breaks down at 6, but reemerges at 7.

What is the actual pattern here?

Theorem 3.7.4 (Fermat's Little Theorem)**.** Let p be a prime. Let $a \in \mathbb{Z}$. Then,

$$a^p \equiv a \bmod p.$$

Proof. We induct on a. This will only cover the case $a \geq 0$, so we will need an extra argument for the case $a < 0$ afterwards.

Base case: The case $a = 0$ is saying $0^p \equiv 0 \bmod p$, which is obvious ($0^p = 0$).

Induction step: Let $a \in \mathbb{N}$. Assume (as the IH) that $a^p \equiv a \bmod p$. We must prove that $(a+1)^p \equiv a+1 \bmod p$.

The binomial formula yields

$$\begin{aligned}
&(a+1)^p \\
&= \underbrace{a^p}_{\substack{\equiv a \bmod p \\ \text{(by the IH)}}} + \underbrace{\binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a}_{\substack{\text{divisible by } p \\ \text{(since the preceding theorem says} \\ \text{that } p \mid \binom{p}{k} \text{ for each } k \in \{1,2,\ldots,p-1\})}} +1 \\
&= a + (\text{a multiple of } p) + 1 \equiv a + 1 \bmod p.
\end{aligned}$$

This completes the induction step.

So we have proved the theorem for all $a \geq 0$.

It remains to prove it for $a < 0$. So let $a < 0$. Set $b := a\%p$. Then, $b \geq 0$, so that $b^p \equiv b \bmod p$ (since we have already proved the theorem for nonnegative integers). However, $b = a\%p \equiv a \bmod p$, so that $b^p \equiv a^p \bmod p$. Hence,

$$a^p \equiv b^p \equiv b \equiv a \bmod p.$$

So the theorem is proved for $a < 0$ as well. (See the notes for details.) □

Remark 3.7.5. The converse of Fermat's Little Theorem is not true: There also exist some non-prime numbers p for which every $a \in \mathbb{Z}$ satisfies $a^p \equiv a \bmod p$. These are called **Carmichael numbers**. One of them is 561.

3.7.5. Prime divisor separation theorem

You can think of the primes as "inseparable" positive integers: They cannot be "broken apart" into two nontrivial factors.

This "inseparability" goes further than that: If a prime number p divides a product ab of two integers, then it must divide a or b (or both). In other words:

Theorem 3.7.6 (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. We shall prove the claim in the following equivalent form: "If $p \nmid a$, then $p \mid b$".

Assume that $p \nmid a$. We must then prove that $p \mid b$.

The friend-or-foe lemma yields that a is either divisible by p or coprime to p. Since a is not divisible by p (because we assumed $p \nmid a$), we thus conclude that a is coprime to p. In other words, p is coprime to a. Hence, the coprime removal theorem lets us conclude $p \mid b$ from $p \mid ab$. So we are done. □

This theorem crucially relies on p being a prime. For instance, it would break for $p = 4$, since $4 \mid 2 \cdot 6$ but $4 \nmid 2$ and $4 \nmid 6$.

We can extend the above theorem to products of several factors:

> **Corollary 3.7.7** (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 words: If a prime divides a product of several integers, then it must divide at least one of its factors.)

Proof. Induct on k. In the base case ($k = 0$), the claim is vacuously true since $p \nmid 1$. In the *induction step* (from k to $k+1$), write $a_1 a_2 \cdots a_k$ as $(a_1 a_2 \cdots a_{k-1})\, a_k$, and use the theorem. □

3.7.6. p-valuations: definition

We will need the following simple lemma:

> **Lemma 3.7.8.** Let p be a prime. Let n be a nonzero integer. Then, there exists a largest $m \in \mathbb{N}$ such that $p^m \mid n$.

Proof. We have $p^0 = 1 \mid n$, so the relation $p^m \mid n$ is always satisfied for $m = 0$.

Every $m > |n|$ satisfies $p^m > p^{|n|} > |n|$, so that $p^m \nmid n$. So there are only finitely many $m \in \mathbb{N}$ satisfying $p^m \mid n$. In particular, there is a largest one.

Alternatively: The relation $p^m \mid n$ means that n can be divided by p at least m times without getting a non-integer. This can clearly not hold for arbitrarily large m, since dividing n by p over and over will eventually produce a non-integer (because each such division decreases $|n|$). So again, there is a last time that it works, i.e., a largest m. □

> **Definition 3.7.9.** 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 $p^m \mid n$. In other words, $v_p(n)$ is the number of times that we can divide n by p without getting a non-integer.
>
> This number $v_p(n)$ is called the ***p*-valuation** (or the ***p*-adic valuation**) of n.
>
> **(b)** We also define $v_p(0)$ (in order for $v_p(n)$ to exist for all $n \in \mathbb{Z}$). Namely, we define it to be ∞. This symbol ∞ is not an actual number, but we shall pretend that it behaves like one. In particular, we can add and compare it to other numbers, following the rules
>
> $$\begin{aligned} k + \infty &= \infty + k = \infty && \text{for all } k \in \mathbb{Z}; \\ \infty + \infty &= \infty; \\ k < \infty &\text{ and } \infty > k && \text{for all } k \in \mathbb{Z}. \end{aligned}$$
>
> (So ∞ acts like a "mythical number that is larger than any actual number".) As we said, ∞ is not really a number, but it plays its role well as long as we

only add and compare. (If we start subtracting, things break: Subtracting ∞ from $0 + \infty = 1 + \infty$ would yield $0 = 1$, which is wrong. So you cannot involve ∞ in subtract.)

Here are some examples:

- We have

$$\begin{aligned} v_3(99) &= 2 && \left(\text{since } 3^2 \mid 99 \text{ but } 3^3 \nmid 99\right); \\ v_3(98) &= 0 && \left(\text{since } 3^0 \mid 98 \text{ but } 3^1 \nmid 98\right); \\ v_3(96) &= 1 && \left(\text{since } 3^1 \mid 96 \text{ but } 3^2 \nmid 96\right); \\ v_3(0) &= \infty. \end{aligned}$$

We can view $v_p(n)$ in yet another way: If p is a prime and n is a positive integer, then $v_p(n)$ is the number of zeroes at the end of the base-p representation of n. For example, the base-2 representation of 344 is 101011000, which has three zeroes at the end, so that $v_2(344) = 3$.

Note that the definition of $v_p(n)$ can be generalized to any integer $p > 1$ instead of p (not just a prime). But most of its useful properties require p to be a prime.

3.7.7. p-valuations: basic properties

Lemma 3.7.10. 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. If $n = 0$, then this is clear (because both $p^i \mid 0 = n$ and $v_p(n) = v_p(0) = \infty \geq i$ hold in this case).

It remains to deal with the case $n \neq 0$. In this case, $v_p(n)$ is defined as the largest $m \in \mathbb{N}$ such that $p^m \mid n$. Thus, in this case,

- if $i \leq v_p(n)$, then $p^i \mid p^{v_p(n)} \mid n$;
- if $i > v_p(n)$, then $p^i \nmid n$.

So we conclude that $p^i \mid n$ if and only if $i \leq v_p(n)$. □

Next, we recall some standard notations: For any two numbers x and y, we let $\min\{x, y\}$ and $\max\{x, y\}$ denote the smallest and the largest of x and y. More generally, if S is any set of numbers, then $\min S$ and $\max S$ denote the smallest and the largest elements of S (if these exist). These notations are extended to ∞ in the obvious way:

$$\min\{k, \infty\} = \min\{\infty, k\} = k \qquad \text{for any } k \in \mathbb{Z} \cup \{\infty\};$$
$$\max\{k, \infty\} = \max\{\infty, k\} = \infty \qquad \text{for any } k \in \mathbb{Z} \cup \{\infty\}.$$

Now, we can state a bunch of important facts about p-valuations:

Theorem 3.7.11 (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 $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$ 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. **(a)** Let $a, b \in \mathbb{Z}$. We must prove that $v_p(ab) = v_p(a) + v_p(b)$.

If $a = 0$, then this boils down to $\infty = \infty + v_p(b)$, which is obvious. Similarly for $b = 0$. Thus, it only remains to handle the case when both a and b are nonzero.

Consider this case. Then, $v_p(a)$ and $v_p(b)$ are nonnegative integers. Let's call them

$$n = v_p(a) \qquad \text{and} \qquad m = v_p(b).$$

Thus, $p^n \mid a$ but $p^{n+1} \nmid a$, and likewise $p^m \mid b$ but $p^{m+1} \nmid b$.

We must prove that $v_p(ab) = n + m$. In other words, we must prove that $p^{n+m} \mid ab$ but $p^{n+m+1} \nmid ab$.

From $p^n \mid a$, we see that $a = p^n x$ for some integer x. This integer x cannot be divisible by p (since otherwise, we would have $x = px'$ for some integer x', and therefore $a = p^n x = p^n p x' = p^{n+1} x'$, which would contradict $p^{n+1} \nmid a$).

So we have written a as $a = p^n x$ for some integer x not divisible by p.

Similarly, we can write b as $b = p^m y$ for some integer y not divisible by p.

Hence, $ab = p^n x \cdot p^m y = p^{n+m} xy$, which immediately yields $p^{n+m} \mid ab$.

Remains to prove that $p^{n+m+1} \nmid ab$. Assume the contrary. Thus, $p^{n+m+1} \mid ab$. Since $ab = p^{n+m} xy$, this rewrites as $p^{n+m+1} \mid p^{n+m} xy$. Cancelling p^{n+m} from this divisibility, we obtain $p \mid xy$. Hence, by the prime divisor separation theorem, $p \mid x$ or $p \mid y$. But this is impossible, since neither x nor y is divisible by p. This contradiction shows that our assumption was false, and thus $p^{n+m+1} \nmid ab$ is true.

From $p^{n+m} \mid ab$ and $p^{n+m+1} \nmid ab$, we obtain $v_p(ab) = n + m = v_p(a) + v_p(b)$, so the proof is complete.

(b) Let $a, b \in \mathbb{Z}$. We must prove $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$.

If $a = 0$, then this is saying $v_p(b) \geq \min\{\infty, v_p(b)\}$, which is obvious. If $b = 0$, then this is obvious for similar reasons. Thus, again, we only need to care about the case when a and b are nonzero. In this case, set $k := \min\{v_p(a), v_p(b)\}$. Then, both a and b are multiples of p^k (since $k \leq v_p(a)$ and $k \leq v_p(b)$). Hence, $a + b$ is also a multiple of p^k. In other words, by the above lemma, $v_p(a+b) \geq k = \min\{v_p(a), v_p(b)\}$, so we are done.

(c) Follows from $p^0 = 1 \mid 1$ and $p^1 = p \nmid 1$.

(d) Follows from $p^1 = p \mid p$ and $p^2 \nmid p$.

(e) Let $q \neq p$ be a prime. Then, $p \nmid q$ (since the only positive divisors of q are 1 and q, but p is neither of them). In other words, $p^1 \nmid q$. But $p^0 = 1 \mid q$. So $v_p(q) = 0$. □

Corollary 3.7.12. Let p be a prime. Then,

$$v_p\left(a_1a_2\cdots a_k\right) = v_p\left(a_1\right) + v_p\left(a_2\right) + \cdots + v_p\left(a_k\right)$$

for any k integers $a_1, a_2, \ldots, a_k$.

Proof. Induct on k. In the base case, use $v_p\left(1\right) = 0$. In the induction step, use part **(a)** of the theorem. □

3.7.8. Back to Hanoi

Proposition 3.7.13. Let $n \in \mathbb{N}$. Recall the strategy for the Tower of Hanoi puzzle with n disks.

Let $k \in \{1, 2, \ldots, 2^n - 1\}$. Then, the k-th move of this strategy moves the $\left(v_2\left(n\right) + 1\right)$-th smallest disk.

This is proved in the notes (§3.6.9). The sequence

$$\begin{aligned}&\left(v_2\left(1\right),\ v_2\left(2\right),\ v_2\left(3\right),\ v_2\left(4\right),\ v_2\left(5\right),\ \ldots\right)\\ &= \left(0,\ 1,\ 0,\ 2,\ 0,\ 1,\ 0,\ 3,\ 0,\ 1,\ 0,\ 2,\ 0,\ 1,\ 0,\ 4,\ \ldots\right)\end{aligned}$$

is known as the **ruler sequence**.

3.7.9. The p-valuation of n!

Theorem 3.7.14 (de Polignac's formula)**.** Let p be a prime. Let $n \in \mathbb{N}$. Then,

$$\begin{aligned}v_p\left(n!\right) &= \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \\ &= \left(n//p^1\right) + \left(n//p^2\right) + \left(n//p^3\right) + \cdots .\end{aligned}$$

Proof idea. First of all, these are infinite sums. In truth, they are finite sums in disguise, because only finitely many of their addends are nonzero. For instance, for $p = 2$ and $n = 13$, we have

$$\begin{aligned}&\left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \\ &= \left\lfloor \frac{13}{2^1} \right\rfloor + \left\lfloor \frac{13}{2^2} \right\rfloor + \left\lfloor \frac{13}{2^3} \right\rfloor + \cdots \\ &= \lfloor 6.5 \rfloor + \lfloor 3.25 \rfloor + \lfloor 1.625 \rfloor + \lfloor 0.8125 \rfloor + \lfloor 0.40625 \rfloor + \cdots \\ &= 6 + 3 + 1 + \underbrace{0 + 0 + 0 + 0 + \cdots}_{\text{Throw these away!}} \\ &= 6 + 3 + 1 = 10.\end{aligned}$$

Moreover, for every positive integer d, we have $\left\lfloor \frac{n}{d} \right\rfloor = n//d$, so that the two sums

$$\begin{aligned} & \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \\ \text{and} \qquad & \left(n//p^1\right) + \left(n//p^2\right) + \left(n//p^3\right) + \cdots \end{aligned}$$

are equal. We thus only need to prove that these two sums equal $v_p(n!)$. In other words, we must 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: For $n = 0$, we must show that $v_p(1) = 0$, which is obvious.

In the *induction step*, we proceed from $n-1$ to n. So we assume (for a fixed integer $n > 0$) that

$$v_p((n-1)!) = \left\lfloor \frac{n-1}{p^1} \right\rfloor + \left\lfloor \frac{n-1}{p^2} \right\rfloor + \left\lfloor \frac{n-1}{p^3} \right\rfloor + \cdots .$$

We must prove that

$$v_p(n!) = \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots .$$

The trick is to show that the left hand sides of these two equations differ by $v_p(n)$, and so do the right hand sides. For the left hand sides, this is easy:

$$\begin{aligned} v_p(n!) &= v_p((n-1)! \cdot n) \qquad && (\text{since } n! = (n-1)! \cdot n) \\ &= v_p((n-1)!) + v_p(n). \end{aligned}$$

For the right hand sides, we recall the birthday lemma:

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

This yields that

$$\begin{aligned} \left\lfloor \frac{n}{p^i} \right\rfloor &= \left\lfloor \frac{n-1}{p^i} \right\rfloor + 1 \qquad && \text{if } i \leq v_p(n); \\ \left\lfloor \frac{n}{p^i} \right\rfloor &= \left\lfloor \frac{n-1}{p^i} \right\rfloor \qquad && \text{if } i > v_p(n). \end{aligned}$$

Details in the notes (Theorem 3.6.15). □

3.7.10. Prime factorization

We are now ready to prove one of the most important properties of primes: the fact that any positive integer can be uniquely decomposed into a product of primes. For instance,

$$200 = 2 \cdot 100 = 2 \cdot 2 \cdot 50 = 2 \cdot 2 \cdot 5 \cdot 10 = \underbrace{2 \cdot 2 \cdot 5 \cdot 2 \cdot 5}_{\text{a product of primes}} .$$

The word "uniquely" here means that any two ways of decomposing a given $n > 0$ into a product of primes are equal up to reordering the factors. For example, $200 = 5 \cdot 5 \cdot 2 \cdot 2 \cdot 2$ counts as the same way.

Let us state this fact in full generality. First, we introduce a name for these decompositions:

Definition 3.7.15. 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 example, $(2, 2, 5, 2, 5)$ and $(5, 5, 2, 2, 2)$ are two prime factorizations of 200. The claim is that any prime factorization of 200 is the same up to the order of its factors, i.e., consists of three 2's and two 5's.

More generally:

Theorem 3.7.16 (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 $(q_1, q_2, \ldots, q_\ell)$ are two prime factorizations 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 this list $(p_1, p_2, \ldots, p_k)$ is $v_p(n)$.

Proof. **(a)** This was proved a while ago, as an example of strong induction.

(c) By the definition of a prime factorization, $n = p_1 p_2 \cdots p_k$. Thus,

$$\begin{aligned}
v_p(n) &= v_p(p_1 p_2 \cdots p_k) \\
&= v_p(p_1) + v_p(p_2) + \cdots + v_p(p_k) \qquad \text{(by the last corollary)} \\
&= \left(\begin{array}{c}\text{a sum of 0's and 1's, where the 1's correspond to} \\ \text{the } p_i\text{'s that equal } p\end{array}\right) \\
&\qquad \left(\begin{array}{c}\text{since } v_p(p) = 1 \text{ and since } v_p(q) = 0 \\ \text{for all primes } q \neq p\end{array}\right) \\
&= (\text{the number of 1's in this sum}) \\
&= (\text{the number of } p_i\text{'s that equal } p) \\
&= (\text{the number of times that } p \text{ appears in } (p_1, p_2, \ldots, p_k)).
\end{aligned}$$

(b) Let $(p_1, p_2, \ldots, p_k)$ and $(q_1, q_2, \ldots, q_\ell)$ be two prime factorizations of n. For any prime p, the number of times that p appears in $(p_1, p_2, \ldots, p_k)$ is $v_p(n)$ (by part **(c)**), but the number of times that p appears in $(q_1, q_2, \ldots, q_\ell)$ is also $v_p(n)$ (by part **(c)** again). Thus, any prime p appears the same number of times in $(p_1, p_2, \ldots, p_k)$ as it does in $(q_1, q_2, \ldots, q_\ell)$. So the two lists $(p_1, p_2, \ldots, p_k)$ and $(q_1, q_2, \ldots, q_\ell)$ contain each prime the same number of times. Thus, the two lists are equal up to order. In other words, one is obtained from the other by reordering the entries. □

3.8. Least common multiples

Least common multiples (short: lcms) are a counterpart to greatest common divisors (gcds).

Definition 3.8.1. Let a and b be two integers.

(a) The **common multiples** of a and b are the integers that are divisible by both a and b simultaneously.

(b) The **least common multiple** (aka the **lowest common multiple**, or just 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 $\operatorname{lcm}(a, b)$.

Some examples:

- We have $\operatorname{lcm}(3, 4) = 12$.

- We have $\operatorname{lcm}(6,4) = 12$.
- We have $\operatorname{lcm}(6,8) = 24$. (In fact, the positive multiples of 8 are $8, 16, 24, \ldots$.)
- We have $\operatorname{lcm}(3,6) = 6$.
- We have $\operatorname{lcm}(0,5) = 0$.
- We have $\operatorname{lcm}(3,-4) = 12$. (In fact, the multiples of -4 are just the multiples of 4.)

Note that the lcm of positive integers is a well-known concept: The lowest common denominator of two fractions is precisely the lcm of their denominators.

Theorem 3.8.2. 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 $\operatorname{lcm}(-a,b) = \operatorname{lcm}(a,b)$ and $\operatorname{lcm}(a,-b) = \operatorname{lcm}(a,b)$.

Proof. **(a)** If a or b is 0, then this is clear by definition.
Otherwise, we need to show that there is a positive common multiple of a and b. To do so, we just notice that $|ab|$ is such a multiple.

(b), **(c)**, **(d)** Obvious.
(e) This is because divisibility does not depend on signs. □

Recall the universal property of the gcd, which says that

$$(m \mid a \text{ and } m \mid b) \iff (m \mid \gcd(a,b)).$$

There is an analogous property for lcms:

Theorem 3.8.3 (universal property of the lcm)**.** Let $a, b, m \in \mathbb{Z}$. Then, we have the equivalence

$$(a \mid m \text{ and } b \mid m) \iff (\operatorname{lcm}(a,b) \mid m).$$

In words: The common multiples of a and b are precisely the multiples of $\operatorname{lcm}(a,b)$.

Proof. $\Longleftarrow$: Assume that $\operatorname{lcm}(a,b) \mid m$. We must prove that $a \mid m$ and $b \mid m$.
We have $a \mid \operatorname{lcm}(a,b) \mid m$, thus $a \mid m$. Similarly, $b \mid m$.
$\Longleftarrow$: Assume that $a \mid m$ and $b \mid m$. We must prove that $\operatorname{lcm}(a,b) \mid m$.

If a or b is 0, then this is easy (since if a or b is 0, then $a \mid m$ and $b \mid m$ entails $m = 0$, so that $\operatorname{lcm}(a,b) \mid 0 = m$). It remains to consider the other case.

In this other case, a and b are nonzero, so that $\operatorname{lcm}(a,b)$ is literally the smallest positive common multiple of a and b. Let us denote it by ℓ. So $\ell = \operatorname{lcm}(a,b) > 0$.

Now, let $q := m//\ell$ and $r := m\%\ell$ be the quotient and the remainder of dividing m by ℓ. Then,

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

From $r \in \{0,1,\ldots,\ell-1\}$, we get $r < \ell$.

From $m = q\ell + r$, we obtain $r = m - q\ell$. Since both m and ℓ are multiples of a (because $a \mid m$ and $\ell = \operatorname{lcm}(a,b)$), the difference $m - q\ell$ is a multiple of a. In other words, r is a multiple of a (since $r = m - q\ell$). Similarly, r is a multiple of b. So r is a common multiple of a and b.

If r was positive, then r would thus be a positive common multiple of a and b, and therefore $r \geq \ell$ since ℓ is the **smallest** positive common multiple of a and b; but this would contradict $r < \ell$. So r cannot be positive. Since $r \in \{0,1,\ldots,\ell-1\}$, this entails that $r = 0$. Thus, $m\%\ell = r = 0$, so that $\ell \mid m$. Since $\ell = \operatorname{lcm}(a,b)$, so this means that $\operatorname{lcm}(a,b) \mid m$. Qed. □

The gcd and the lcm of two integers are related by the following formula:

Theorem 3.8.4. Let a and b be two integers. Then,

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|.$$

Proof sketch. (See a reference in the notes for a detailed proof.)

The case when a or b is 0 is easy. Consider the other case. Argue that $\dfrac{ab}{\gcd(a,b)}$ is a common multiple of a and b, and thus (by the universal property of the lcm) a multiple of $\operatorname{lcm}(a,b)$. Thus,

$$\operatorname{lcm}(a,b) \mid \frac{ab}{\gcd(a,b)}, \qquad \text{and thus}$$
$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) \mid ab.$$

On the other hand, $\dfrac{ab}{\operatorname{lcm}(a,b)}$ is an integer (by the universal property of the lcm) and divides $\gcd(a,b)$ (by the universal property of the gcd, since it divides both a and b). Thus,

$$\frac{ab}{\operatorname{lcm}(a,b)} \mid \gcd(a,b), \qquad \text{and thus}$$
$$ab \mid \gcd(a,b) \cdot \operatorname{lcm}(a,b).$$

Now recall that if two integers x and y mutually divide each other (i.e., satisfy $x \mid y$ and $y \mid x$), then $|x| = |y|$. Hence, from

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) \mid ab \qquad \text{and} \qquad ab \mid \gcd(a,b) \cdot \operatorname{lcm}(a,b),$$

we obtain

$$|\gcd(a,b) \cdot \operatorname{lcm}(a,b)| = |ab|.$$

The LHS does not need $||$ brackets because the thing inside is already ≥ 0. □

Both gcds and lcms have easily computable p-valuations:

Theorem 3.8.5. Let p be a prime. Let a and b be two integers. Then,

$$v_p(\gcd(a,b)) = \min\{v_p(a),\ v_p(b)\};$$
$$v_p(\operatorname{lcm}(a,b)) = \max\{v_p(a),\ v_p(b)\}.$$

Proof. See the reference in the notes. Or do it yourself using the universal properties and using the properties of p-valuations. □

This theorem gives an easy way to compute $\gcd(a,b)$ and $\operatorname{lcm}(a,b)$ if you know the prime factorizations of a and b. For instance, knowing that $54 = 2^1 \cdot 3^3$ and $12 = 2^2 \cdot 3^1$, we obtain

$$\gcd(54,\ 12) = 2^1 \cdot 3^1 = 6;$$
$$\operatorname{lcm}(54,\ 12) = 2^2 \cdot 3^3 = 108.$$

If you don't know prime factorizations of a and b, then the best way to compute $\gcd(a,b)$ and $\operatorname{lcm}(a,b)$ is to first compute $\gcd(a,b)$ by the Euclidean algorithm, and then solve the equation

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|$$

for $\operatorname{lcm}(a,b)$.

Finally, let me notice that gcds and lcms can also be defined for multiple (more than two) numbers. They satisfy most of the same properties, except that the formula

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|$$

becomes more complicated (not $\gcd(a,b,c) \cdot \operatorname{lcm}(a,b,c) = |abc|$ but $\gcd(a,b,c) \cdot \operatorname{lcm}(bc,ca,ab) = |abc|$). See the notes for a reference.

3.9. Sylvester's $xa + yb$ theorem (aka Chicken McNugget theorem)

Now we recall the coin problem from Chapter 1: what denominations can be paid with 3-cent coins and 5-cent coins without taking change.

Let us generalize this problem: Given $a, b \in \mathbb{N}$, we want to know what denominations can be paid with a-cent coins and b-cent coins without taking change. As a warmup, let us solve this problem with change as well. We introduce notations first.

For this entire section, we fix two positive integers a and b.

Definition 3.9.1. (a) A **$\mathbb{Z}$-linear combination** (short: **$\mathbb{Z}$-LC**) 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 using a-cent coins and b-cent coins if you can take change.

(b) An **$\mathbb{N}$-linear combination** (short: **$\mathbb{N}$-LC**) 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 using a-cent coins and b-cent coins without taking change.

The result we found back a while ago is that the $\mathbb{N}$-LCs of 3 and 5 are

$$0,\ 3,\ 5,\ 6,\ \underbrace{8,\ 9,\ 10,\ \ldots}_{\text{all integers } n \geq 8}.$$

A similar (but more exhausting) analysis shows that the $\mathbb{N}$-LCs of 5 and 9 are

$$0,\ 5,\ 9,\ 10,\ 14,\ 15,\ 18,\ 19,\ 20,\ 23,\ 24,\ 25,\ 27,\ 28,\ 29,\ 30,\ \underbrace{32,\ 33,\ 34,\ \ldots}_{\text{all integers } n \geq 32}.$$

What can we say about the general case? We see some patterns in the above two examples:

- There is a threshold value after which every denomination can be paid.
- Exactly half of the nonnegative integers below this threshold value can be paid.
- The threshold value is a power of 2.

The first two of these patterns generalize; the third does not. However, there is a hidden requirement here: a and b need to be coprime. (If a and b have a common divisor $d > 1$, then any $\mathbb{N}$-LC of a and b is also a multiple of d, and thus non-multiples of d cannot be paid.) But the coprime case is the only interesting case, since in the other case you can just replace a and b by $\dfrac{a}{\gcd(a,b)}$ and $\dfrac{b}{\gcd(a,b)}$ and all the $\mathbb{N}$-LCs of a and b will also be shrunk by $\gcd(a,b)$.

In this coprime case, the following result (by J. J. Sylvester, 1884) tells us that our first two patterns generalize:

Theorem 3.9.2 (Sylvester's two-coin theorem)**.** Assume that the two positive integers a and b are coprime. Then:

(a) Every integer $n > ab - a - b$ is an $\mathbb{N}$-LC of a and b.

(b) The number $ab - a - b$ is **not** an $\mathbb{N}$-LC of a and b.

(c) Among the first $ab - a - b + 1$ nonnegative integers $0, 1, \ldots, ab - a - b$, exactly half are $\mathbb{N}$-LCs 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 $\mathbb{N}$-LC of a and b.

This theorem does not characterize the $\mathbb{N}$-LCs of a and b are completely, but it makes their characterization into a finite problem that you can give to a computer (since there are only finitely many values $1, 2, \ldots, ab - a - b - 1$ to check).

A proof of this theorem can be found in the notes (§3.8).

For comparison:

Theorem 3.9.3. The $\mathbb{Z}$-LCs of a and b are just the multiples of $\gcd(a,b)$.

Proof. Easy using the Bezout theorem. (See the notes.) □

3.10. A bit of cryptography

Cryptography is the study of ciphers, i.e., methods of encrypting data (usually text). It is a whole science in itself (not part of mathematics, but using a lot of mathematics).

We will see an ancient (Roman) and a modern (20th century) cipher. There are many more, and you can learn about them from various books, some of which are cited in the notes. Most ciphers are based on number theory.

3.10.1. Caesarian ciphers (alphabet rotation)

We begin with an encryption algorithm used by Julius Caesar to encrypt military communications. We assume that our messages are text and are written in the modern English alphabet, all in uppercase.

The modern English alphabet has 26 letters, and we assign a number to each of them:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

.

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Thus, each letter corresponds to a unique number in the set $\{0, 1, \ldots, 25\}$. For instance, F $\cong$ 5 and X $\cong$ 23 and N $\cong$ 13. This is called **numeric encoding** of letters.

A word is just a finite list of letters, and thus can be encoded as a finite list of numbers (in the set $\{0, 1, \ldots, 25\}$) using the numeric encoding. For instance,

$$\text{KITTEN} \rightarrow (\text{K, I, T, T, E, N}) \rightarrow (10,\ 8,\ 19,\ 19,\ 4,\ 13)\,.$$

Conversely, any finite list of numbers (in this set) can be decoded into a word (not necessarily a meaningful one). For instance, $(17,\ 0,\ 19) \rightarrow$ RAT.

Now we can formulate Caesar's algorithm, which is nowadays known as the "Caesarian cipher ROT$_3$":

Caesarian cipher ROT$_3$**:** To encrypt a word, proceed as follows:

1. Encode the word as a finite list of numbers $(a_1, a_2, \ldots, a_n)$ using the numeric encoding.

2. Replace each number a_i in this list by $(a_i + 3)\,\%26$.

3. Decode the resulting list back into a word.

For example,

$$\text{CRAZY} \rightarrow (2,\ 17,\ 0,\ 25,\ 24) \rightarrow (5,\ 20,\ 3,\ 2,\ 1) \rightarrow \text{FUDCB}.$$

In other words, if we view the alphabet as being wrapped around a dial, then ROT$_3$ shifts each letter by 3 steps along this dial.

How do we decrypt a word encrypted using ROT$_3$? Using the following algorithm:

Caesarian cipher ROT$_{-3}$**:** To decrypt a word, proceed as follows:

1. Encode the word as a finite list of numbers $(a_1, a_2, \ldots, a_n)$ using the numeric encoding.

2. Replace each number a_i in this list by $(a_i - 3)\,\%26$.

3. Decode the resulting list back into a word.

More generally, for any integer k, we can define the ROT_k encryption/decryption algorithm as follows:

Caesarian cipher ROT_k**:** To en/decrypt a word using a given integer k, proceed as follows:

1. Encode the word as a finite list of numbers $(a_1, a_2, \ldots, a_n)$ using the numeric encoding.
2. Replace each number a_i in this list by $(a_i + k)\,\%26$.
3. Decode the resulting list back into a word.

We can easily see the following:

- The ROT_k algorithm is undone by the ROT_{-k} algorithm. In other words, a word encrypted using ROT_k will always be decrypted using ROT_{-k}.
- The ROT_0 algorithm does nothing: The encrypted word will be just the original word.
- The ROT_{26} algorithm also does nothing: $(a + 26)\,\%26 = a$ for each $a \in \{0, 1, \ldots, 25\}$.
- More generally, if two integers k and ℓ satisfy $k \equiv \ell \mod 26$, then $\text{ROT}_k = \text{ROT}_\ell$. Thus, there are only 26 distinct Caesarian ciphers, namely

  $$\text{ROT}_0, \ \text{ROT}_1, \ \text{ROT}_2, \ \ldots, \ \text{ROT}_{25}.$$

  Any other ROT_k is just a duplicate of one of these 26. Out of these 26, only 25 are useful as ciphers, since ROT_0 does nothing.
- If k and ℓ are two integers, then applying ROT_k and ROT_ℓ consecutively yields the same result as just applying $\text{ROT}_{k+\ell}$.
- The algorithm ROT_{13} undoes itself – i.e., a word encrypted using ROT_{13} can be decrypted by applying ROT_{13} again. Indeed, applying ROT_{13} and ROT_{13} consecutively gives $\text{ROT}_{13+13} = \text{ROT}_{26} = \text{ROT}_0$, which does nothing.

These observations are obvious if you view ROT_k as shifting each letter by k steps on the alphabet dial. If you want to prove them rigorously using the remainder definition, you need to recall the facts that

- two integers a and b satisfy $a \equiv b \mod 26$ if and only if $a\%26 = b\%26$, and
- the remainder $a\%26$ is the unique integer in $\{0, 1, \ldots, 25\}$ that is congruent to a modulo 26.

For example, to prove that ROT_{-k} undoes ROT_k, you need to show that if $a \in \{0,1,\ldots,25\}$ and $b = (a+k)\,\%26$, then $a = (b-k)\,\%26$. This can be done as follows:

$$\begin{aligned} b = (a+k)\,\%26 &\Longrightarrow b \equiv a + k \bmod 26 \\ &\Longrightarrow b - k \equiv a \bmod 26 \\ &\Longrightarrow a \equiv b - k \bmod 26 \\ &\Longrightarrow a = (b-k)\,\%26 \end{aligned}$$

since $a \in \{0,1,\ldots,25\}$.

3.10.2. Keys and ciphers

Caesarian ciphers are not very secure. They are one-trick ponies: Once your enemy knows the cipher, he can decrypt anything you encrypt. Even if he does not know the k, he can easily find it given a bit of ciphertext. In fact, there are only 25 reasonable Caesarian ciphers

$$\operatorname{ROT}_1, \ \operatorname{ROT}_2, \ \ldots, \ \operatorname{ROT}_{25},$$

and you can easily tell which one I am using by trying to decrypt using each one and seeing which of the results will not be gibberish. In modern terms, the **key size** is too small. So we need better methods. Next time we will see some.

Example: Let's say you know that the ROT_k-encrypted ciphertext is "BPQA QA VWB BPM EIG", but you don't know what k is. How do you decrypt the text?

You just apply each of $\operatorname{ROT}_0, \ \operatorname{ROT}_1, \ \operatorname{ROT}_2, \ \ldots, \ \operatorname{ROT}_{25}$, and see which of them results in non-gibberish text. The answer is ROT_{18}, and the text you get is "THIS IS NOT THE WAY". So the k was -18 or, equivalently, 8.

So Caesarian ciphers are a bad cipher, at least for two reasons: The key size is too small (26), and the encryption algorithm is not "chaotic" enough (e.g., each letter is encrypted by the same rule). Over the centuries, people have invented better ciphers, which solve one or the other of these reasons. Some examples:

- **Monoalphabetic cipher:** Instead of shifting each letter, we apply an arbitrary permutation to the alphabet. For instance, let me choose the permutation

A	B	C	D	E	F	G	H	I	J	K	L	M
O	E	I	L	R	Q	A	X	V	F	K	C	T

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	Y	B	S	J	P	M	G	W	H	D	U	Z

.

Thus, for example, the word KITTEN becomes KVMMRN.

This cipher has a much bigger key size than a Caesarian cipher, since the keys are now the permutations of the whole alphabet, and (as we will soon see) there are $26! = 403\,291\,461\,126\,605\,635\,584\,000\,000$ of them. You cannot just try them all and see which of them works.

Nevertheless, if your text is long enough, the "lack of chaos" in this method will eventually betray you. For instance, equal letters in the cipher text come from equal letters in the plain text; the frequencies of the letters have been preserved even if permuted (and this is useful, since some letters are much more frequent than others); certain pairs of letters rarely appear consecutively; and so on.

Certain variants have been suggested, which are less prone to some of these issues.

- **Viginere code:** This like a Caesarian cipher, except that each letter gets a different k added to it, depending on its position. So the key is an infinite (or sufficiently long) sequence

$$(k_1, k_2, k_3, \ldots) \text{ of integers in } \{0, 1, \ldots, 25\} \text{ (or any integers).}$$

To encrypt a word, you encode it as a sequence $(a_1, a_2, \ldots, a_n)$ of numbers; then you replace each number a_i by $(a_i + k_i)\,\%26$; then you decode the resulting sequence back into a word.

This cipher is actually unbreakable if the key $(k_1, k_2, k_3, \ldots)$ really is a random sequence of arbitrary numbers in $\{0, 1, \ldots, 25\}$. However, to achieve this in practice, you need a **codebook** – i.e., a book full of random letters in a well-defined order. The sender and the receiver must both have a copy of the codebook. The total length of the codebook should be at least as large (or at least comparable to) the total length of the text the sender wants to send. This makes the method impractical in many situations.

If you "cheat" – e.g., if you repeat a key, i.e. if you pick a periodic sequence $(k_1, k_2, k_3, \ldots)$ – then the cipher quickly becomes breakable.

Many other techniques have been developed over the centuries to keep information secure. See Simon Singh's "Code Book" for the history and for many examples.

3.10.3. The RSA cipher

All the methods discussed above are **classical ciphers**. Generally, any cipher constructed before the 20th century is called **classical**. These ciphers have one thing in common: They can be used (for encryption and decryption) with pen and paper, without the use of computers. In the mid-20th century, computers came along, and with them a new generation of ciphers, which require computers to encrypt/decrypt text with. These are called **modern ciphers**.

With computers, basically all classical ciphers are breakable (unless the ciphertext is too short). Breaking classical ciphers was one of the reasons why computers were developed during WWII.

We will show one "simple" example of a modern cipher, namely the **RSA cipher** (invented in the 1970s/80s by Rivest, Shamir and Adleman). It is again based on division with remainders and modular arithmetic.

One interesting thing about the RSA cipher is that it works in a less fair-weather situation than most classical ciphers. In a classical cipher, usually, the sender and the receiver must have agreed on the key (e.g., the k in a Caesarian cipher) secretly. If the eavesdropper has been able to listen to this agreement, he will know the key and the cipher will be useless. In contrast, in the RSA cipher, the parties can agree on their keys even over a completely public channel!

Here is how RSA works. Assume that Albert and Julia are communicating over a public channel (e.g., the Internet). Julia wants to send Albert a message that no eavesdropper will understand. But Albert and Julia have not exchanged keys in advance. How can they communicate secretly?

Setup:

- Julia tells Albert (over the channel) that she wants to communicate and thus he should start creating keys.
- Albert generates two distinct large and sufficiently random primes p and q.

  [How? "Sufficiently random" numbers can be created in many ways, e.g., using Geiger counters or other ways to observe physical processes. Sooner or later you will find a prime number. To check whether a given number is prime, there are several reasonably fast algorithms – e.g., the Solovay–Strassen test.]
- Albert computes the product $m = pq$. This number m (called the **modulus)** he makes public.

  [Note that it is hard to reconstruct p and q from m. At least, no fast algorithm is known to factor a large number into primes. Maybe someone will find one and the whole cipher will get broken.]
- Albert computes the product $\ell = (p-1)(q-1)$, but keeps this private.
- Albert randomly picks an integer $e \in \{2, 3, \ldots, \ell - 1\}$ that is coprime to ℓ.

  [Again, he can do this by picking random numbers. Sooner or later, he will find one that is coprime to ℓ. To check coprimality quickly, he can compute $\gcd(e, \ell)$ by the Euclidean algorithm.]

- Albert computes a positive integer d such that $ed \equiv 1 \mod \ell$.

  [How? We have $1 = \gcd(e, \ell) = xe + y\ell$ for some integers x and y, by Bezout's theorem. These x and y can be computed by the extended Euclidean algorithm. Then, $1 = xe + y\ell \equiv xe = ex \mod \ell$. So Albert can just take $d = x$.]

- Albert publishes the pair (e, m) as his **public key**.

- We assume that the message that Julia wants to send to Albert is an element of $\{0, 1, \ldots, m-1\}$. (If the message is longer, she just breaks it into chunks of size m and encrypt each chunk separately.)

Encrypting a message:
If Julia wants to send a message $a \in \{0, 1, \ldots, m-1\}$ to Albert, she just sends $a^e \% m$. In other words, she encrypts her message by taking it to the e-th power and taking its remainder upon division by m.

[How to compute this? a^e will often be a huge number. However, $a^e \% m$ can easily be computed without having to compute a^e. For instance,

$$\begin{aligned} a^3 \% m &= \left(\left(a^2 \% m\right) a\right) \% m; \\ a^4 \% m &= \left(\left(\left(a^2 \% m\right) a\right) \% m\right) a \% m \\ &= \left(a^2 \% m\right)^2 \% m; \\ &\ldots. \end{aligned}$$

In particular, you can use binary exponentiation, and each time you encounter a number larger than m, you replace it by its remainder upon division by m.]

Decrypting a message:
When Albert receives an encrypted message $b \in \{0, 1, \ldots, m-1\}$, he decrypts it by taking $b^d \% m$.

Why does this work? It boils down to the following fact:

Proposition 3.10.1 (correctness of RSA)**.** Let p and q be two distinct primes. Let $m = pq$ and $\ell = (p-1)(q-1)$. Let e and d be two positive integers such that $ed \equiv 1 \mod \ell$. Let $a, b \in \{0, 1, \ldots, m-1\}$ be such that $b = a^e \% m$. Then, $a = b^d \% m$.

To prove this proposition, we need the following lemma:

Lemma 3.10.2. Let p and q be two distinct primes. Let N be a positive integer such that $N \equiv 1 \mod (p-1)(q-1)$. Let a be any integer. Then,

$$a^N \equiv a \mod pq.$$

> **Example 3.10.3.** Let $p = 3$ and $q = 5$ and $N = 9$ (this does satisfy $N \equiv 1 \mod (p-1)(q-1)$). Then, the lemma says that
> $$a^9 \equiv a \mod 15.$$

Proof of the lemma. The primes p and q are distinct, and therefore coprime (why?). Our goal is to prove the congruence $a^N \equiv a \mod pq$, that is, the divisibility $pq \mid a^N - a$. By the coprime divisors theorem, this would follow if we can show the two divisibilities $p \mid a^N - a$ and $q \mid a^N - a$ (since p and q are coprime). So let us prove these two divisibilities.

Specifically, we will only prove $p \mid a^N - a$, since the proof of $q \mid a^N - a$. In other words, we will prove $a^N \equiv a \mod p$.

Now $N \equiv 1 \mod (p-1)(q-1)$, so that $(p-1)(q-1) \mid N-1$. Hence,

$$p-1 \mid (p-1)(q-1) \mid N-1.$$

So $N - 1 = (p-1)c$ for some integer c. Consider this c. Easily, $c \geq 0$. So $N = (p-1)c + 1$.

For example, assume that $c = 4$. Thus, $N = (p-1) \cdot 4 + 1$, so

$$\begin{aligned} a^N = a^{(p-1)\cdot 4+1} &= a^{p-1}a^{p-1}a^{p-1} \underbrace{a^{p-1}a}_{\substack{=a^p \equiv a \mod p \\ \text{(by Fermat's Little Theorem)}}} \\ &\equiv a^{p-1}a^{p-1} \underbrace{a^{p-1}a}_{\substack{=a^p \equiv a \mod p \\ \text{(by Fermat's Little Theorem)}}} \\ &\equiv a^{p-1} \underbrace{a^{p-1}a}_{\substack{=a^p \equiv a \mod p \\ \text{(by Fermat's Little Theorem)}}} \\ &\equiv \underbrace{a^{p-1}a}_{\substack{=a^p \equiv a \mod p \\ \text{(by Fermat's Little Theorem)}}} \equiv a \mod p. \end{aligned}$$

The same argument works for any c: We have

$$\begin{aligned} a^N = a^{(p-1)c+1} &= a^{p-1}a^{p-1} \cdots a^{p-1} \underbrace{a^{p-1}a}_{\substack{=a^p \equiv a \mod p \\ \text{(by Fermat's Little Theorem)}}} \\ &\equiv a^{p-1}a^{p-1} \cdots \underbrace{a^{p-1}a}_{\substack{=a^p \equiv a \mod p \\ \text{(by Fermat's Little Theorem)}}} \qquad \text{(same product with one fewer factor)} \\ &\equiv a^{p-1}a^{p-1} \cdots a^{p-1}a \qquad \text{(same product with one fewer factor)} \\ &\equiv \cdots \equiv a \mod p. \end{aligned}$$

So we have shown that $a^N \equiv a \mod p$, qed. □

Proof of the proposition. We have $b = a^e \% m \equiv a^e \mod m$. Taking this congruence to the d-th power, we find

$$b^d \equiv (a^e)^d = a^{ed} \mod m.$$

But $ed \equiv 1 \mod \ell$. In other words, $ed \equiv 1 \mod (p-1)(q-1)$. So the lemma (applied to $N = ed$) yields

$$\begin{aligned} a^{ed} &\equiv a \mod pq, \qquad \text{that is,} \\ a^{ed} &\equiv a \mod m. \end{aligned}$$

Thus, $b^d \equiv a^{ed} \equiv a \mod m$. Thus, $b^d \% m = a \% m = a$, qed. □

In practice, for RSA to be reasonably secure, you need to apply it "right", in particular

- making sure that your random primes p and q really are random;
- avoiding certain "unsafe" primes;
- not reusing p without reusing q.

The RSA cipher is symmetric: If Albert wants to respond to Julia, he can use his decryption method as encryption, and Julia can do similarly.

RSA can be used not just for secret communications, but also for authentification. As I said, it is essentially secure by modern standards. Nevertheless, better ciphers have been invented, such as elliptic curve cryptography, which is roughly the same idea but working with more complicated structures instead of numbers in $\{0, 1, \ldots, m-1\}$. See a real course on cryptography to learn about those.

4. An informal introduction to enumeration

Enumeration is a fancy word for counting – i.e., answering questions of the form "how many things of a certain type are there?". Here are examples of such questions:

- How many ways are there to choose 3 odd integers between 0 and 20, if the order matters? The answer is 1000.
- How many ways are there to choose 3 odd integers between 0 and 20, if the order does not matter? The answer is 220.

- How many ways are there to choose 3 distinct odd integers between 0 and 20, if the order matters? The answer is 720.
- How many ways are there to choose 3 distinct odd integers between 0 and 20, if the order does not matter? The answer is 120.
- How many prime factorizations does 200 have (counting different orderings as distinct)? The answer is 10.
- How many ways are there to tile a 2×15-rectangle with dominos? The answer is 987.
- How many addends do you get when you expand the product $(a+b)(c+d+e)(f+g)$? The answer is $2 \cdot 3 \cdot 2 = 12$.
- How many positive divisors does 24 have? Let's list them: $1, 2, 3, 4, 6, 8, 12, 24$. So there are 8.

We will first solve a few basic counting problems informally, and then (in the next chapter) make the underlying concepts rigorous, and finally come back to solve more counting problems.

4.1. A refresher on sets

The notion of a set is one of the most fundamental things in mathematics, and it cannot be formally defined.

Informally, a **set** is a collection of objects (numbers, matrices, functions, or other sets, or whatever else comes to your mind) that knows which objects it contains and which it doesn't.

That is, if S is a set and p is any object, then S can either contain p (in which case we write $p \in S$) or not contain p (in which case we write $p \notin S$). 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 or infinite (i.e., contain finitely or infinitely many elements). It can be empty (i.e., containing nothing) or nonempty (i.e., containing something).

An example of a set is the set of all odd integers. This set contains each odd integer, but nothing else. Generally, "the set of X" means the set that contains X and nothing else.

A finite set can be written by listing its elements. For example, the set of all odd integers between 0 and 10 can be written as

$$\{1,3,5,7,9\}.$$

The symbols $\{$ and $\}$ around the list are known as **set braces**; they signify that whatever stands between them goes into the set.

Some more examples of finite sets are

$$\begin{aligned}
&\{1,2,3,4,5\}\,, \\
&\{1,2\}\,, \\
&\{1\} \qquad \text{(this set only contains the element 1)}\,, \\
&\{\} \qquad \text{(the empty set, also denoted } \varnothing\text{)}\,, \\
&\{1,2,\ldots,1000\} \qquad \left(\begin{array}{c}\text{the "} \ldots \text{" refers to a pattern that} \\ \text{should be clear from the context}\end{array}\right).
\end{aligned}$$

Some infinite sets can also be written in this form:

$$\begin{aligned}
&\{1,2,3,\ldots\} \qquad \text{(this is the set of all positive integers)}\,, \\
&\{0,1,2,\ldots\} \qquad \text{(this is the set of all nonnegative integers)}\,, \\
&\{4,5,6,\ldots\} \qquad \text{(this is the set of all integers } \geq 4\text{)}\,, \\
&\{-1,-2,-3,\ldots\} \qquad \text{(this is the set of all negative integers)}\,, \\
&\{\ldots,-2,-1,0,1,2,\ldots\} \qquad \text{(this is the set of all integers)}\,.
\end{aligned}$$

Some other infinite sets cannot be written in this form. For example, how would you list all rational numbers?

Another way to describe a set is simply by putting a description of its elements in set braces. For example,

$$\begin{aligned}
&\{\text{all integers}\} \qquad \text{(this is the set of all integers)}\,, \\
&\{\text{all integers between 3 and 9 inclusive}\}\,, \\
&\{\text{all real numbers}\}\,.
\end{aligned}$$

Often, you want to define a set that contains all things of a certain type that satisfy a certain condition. For example, let's say you want all integers x that satisfy $x^2 < 20$. The notation for this is

$$\left\{ x \text{ is an integer} \ \mid \ x^2 < 20 \right\}.$$

The vertical bar $|$ here should be read as "such that" (don't mistake it for a divisibility sign). The part before this bar tells you what things you are considering. The part after this bar imposes a condition (or several) on these things. The result is the set of all things that satisfy this condition. For instance,

$$\begin{aligned}
&\left\{ x \text{ is an integer} \ \mid \ x^2 < 20 \right\} \\
&= \{\text{all integers whose squares are smaller than } 20\} \\
&= \{-4,-3,-2,-1,0,1,2,3,4\}\,.
\end{aligned}$$

Some authors put a colon : instead of the vertical bar $|$.

Some sets have standard names:

$$\begin{aligned}
\mathbb{Z} &= \{\text{all integers}\} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}\,; \\
\mathbb{N} &= \{\text{all nonnegative integers}\} = \{0, 1, 2, \ldots\}\,; \\
\mathbb{Q} &= \{\text{all rational numbers}\}\,; \\
\mathbb{R} &= \{\text{all real numbers}\}\,; \\
\mathbb{C} &= \{\text{all complex numbers}\}\,; \\
\varnothing &= \{\} \qquad\qquad (\text{this is the empty set})\,.
\end{aligned}$$

Using these notations, we can rewrite

$$\left\{x \text{ is an integer} \ \mid \ x^2 < 20\right\} \text{ as } \left\{x \in \mathbb{Z} \ \mid \ x^2 < 20\right\}.$$

Yet another way of defining sets is when you let a variable range over a given set and collect certain derived quantities. For instance,

$$\left\{x^2 + 2 \ \mid \ x \in \{1, 3, 5, 7, 9\}\right\}$$

means the set whose elements are the numbers $x^2 + 2$ for all $x \in \{1, 3, 5, 7, 9\}$. Explicitly,

$$\begin{aligned}
&\left\{x^2 + 2 \ \mid \ x \in \{1, 3, 5, 7, 9\}\right\} \\
&= \left\{1^2 + 2,\ 3^2 + 2,\ 5^2 + 2,\ 7^2 + 2,\ 9^2 + 2\right\} \\
&= \{3,\ 11,\ 27,\ 51,\ 83\}\,.
\end{aligned}$$

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 of this:

$$\begin{aligned}
\left\{\frac{x+1}{x} \mid x \in \{1, 2, 3, 4\}\right\} &= \left\{\frac{1+1}{1}, \frac{2+1}{2}, \frac{3+1}{3}, \frac{4+1}{4}\right\} \\
&= \left\{2, \frac{3}{2}, \frac{4}{3}, \frac{5}{4}\right\}
\end{aligned}$$

and

$$\begin{aligned}
\left\{x^2 \% 5 \ \mid \ x \in \mathbb{N}\right\} &= \left\{0^2\%5,\ 1^2\%5,\ 2^2\%5,\ 3^2\%5,\ 4^2\%5,\ 5^2\%5,\ 6^2\%5,\ \ldots\right\} \\
&= \{0,\ 1,\ 4,\ 4,\ 1,\ 0,\ 1,\ 4,\ 4,\ \ldots\} \\
&= \{0, 1, 4\}
\end{aligned}$$

(since the only elements are 0, 1 and 4).

Let me stress once again that a set cannot contain an element more than once, and does not come with a specified order on its elements. So

$$\{1,2\} = \{2,1\} = \{1,2,1\} = \{2,1,1,2,1,2,1,1,1,2\}.$$

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 each 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 each element of B is an element of A. This is equivalent to $B \subseteq A$.

(c) We say that $A = B$ if the sets A and B contain the same elements. This is tantamount to saying that both $A \subseteq B$ and $A \supseteq B$.

(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.)

(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

$$\begin{aligned} A \setminus B &:= \{\text{all elements that are contained in } A \text{ but not in } B\} \\ &= \{x \mid x \in A \text{ and } x \notin B\} = \{x \in A \mid x \notin B\}. \end{aligned}$$

Some authors denote this by $A - B$.

(g) We say that A and B are **disjoint** if $A \cap B = \varnothing$ (that is, A and B have no elements in common).

For example,

$$\begin{aligned} \{3,5,7\} &\subseteq \{1,2,3,4,5,6,7\}, \\ \{1,2,3,4,5,6,7\} &\supseteq \{3,5,7\}, \\ \text{we } \textbf{don't} \text{ have } \{3,5,7\} &\subseteq \{1,2,3,4,5,6\}, \\ \{1,2,3\} &= \{3,2,1\}, \\ \{1,3,5\} \cup \{3,6\} &= \{1,3,5,3,6\} = \{1,3,5,6\}, \\ \{1,3,5\} \cap \{3,6\} &= \{3\}, \\ \{1,3,5\} \setminus \{3,6\} &= \{1,5\}, \\ \{3,6\} \setminus \{1,3,5\} &= \{6\}, \\ \mathbb{Z} \setminus \mathbb{N} &= \{\text{all negative integers}\} = \{-1,-2,-3,\ldots\}. \end{aligned}$$

Moreover, the sets $\{1,2,4\}$ and $\{3,5\}$ are disjoint, since $\{1,2,4\} \cap \{3,5\} = \varnothing$.

Definition 4.1.2. Several sets $A_1, A_2, \ldots, A_k$ are said to be **disjoint** if any two of them (not counting a set and itself) are disjoint, i.e., if $A_i \cap A_j = \varnothing$ for all $i < j$.

For example, the three sets $\{1,6\}$, $\{2,7\}$, $\{3,4\}$ are disjoint, but the three sets $\{1,6\}$, $\{2,7\}$, $\{3,6\}$ are not (since $\{1,6\} \cap \{3,6\} \neq \varnothing$).

4.2. Counting, informally

Now let us see how the elements of a set can be counted. We have no rigorous definition of counting yet, so we will be working somewhat informally, but once we find that definition (in two chapters), all our arguments will become rigorous with little changes.

For example, the set of all odd integers between 0 and 10 has 5 elements, which we can list directly: they are $1,3,5,7,9$. More generally:

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 (inclusively).

Informal proof. The equality $(n+1)\,//\,2 = \left\lfloor \dfrac{n+1}{2} \right\rfloor$ follows from something we have done a while ago ($n//d = \left\lfloor \dfrac{n}{d} \right\rfloor$). It remains to prove that there are exactly $\left\lfloor \dfrac{n+1}{2} \right\rfloor$ many odd integers between 0 and n.

We will prove this claim by induction on n:

Base case: For $n = 0$, the claim says that there are exactly $\left\lfloor \dfrac{0+1}{2} \right\rfloor$ many odd integers between 0 and 0. This is true, since $\left\lfloor \dfrac{0+1}{2} \right\rfloor = 0$ is really the # of 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 $\left\lfloor \dfrac{n}{2} \right\rfloor$ many odd integers between 0 and $n-1$. Our goal is to prove that our claim holds for n, i.e., that there are exactly $\left\lfloor \dfrac{n+1}{2} \right\rfloor$ many odd integers between 0 and n.

In other words, our IH is that

$$(\text{\# of odd integers between 0 and } n-1) = \left\lfloor \frac{n}{2} \right\rfloor,$$

and our goal is to show 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.

Consider Case 1. Here, n is even. Thus, n is not odd. Therefore, the odd integers between 0 and n are exactly the odd integers between 0 and $n-1$ (since the newcomer n does not qualify as odd). Thus,

$$\begin{aligned}
&(\text{\# of odd integers between 0 and } n) \\
&= (\text{\# of odd integers between 0 and } n-1) \\
&= \left\lfloor \frac{n}{2} \right\rfloor \qquad \text{(by the IH)} \\
&= \left\lfloor \frac{n+1}{2} \right\rfloor \qquad \text{(by the birthday lemma)}.
\end{aligned}$$

So the goal is proved in Case 1.

Now consider Case 2. Here, n is odd. Therefore, the odd integers between 0 and n are the odd integers between 0 and $n-1$ along with the new integer n. Thus,

$$\begin{aligned}
&(\text{\# of odd integers between 0 and } n) \\
&= (\text{\# of odd integers between 0 and } n-1) + 1 \\
&= \left\lfloor \frac{n}{2} \right\rfloor + 1 \qquad \text{(by the IH)} \\
&= \left\lfloor \frac{n+1}{2} \right\rfloor \qquad \text{(by the birthday lemma)}.
\end{aligned}$$

So the goal is achieved in Case 2 as well.

Thus, we are done in both cases, so the induction step is complete. □

Note: We only called this proof "informal" since we don't yet know what counting means. Other than that, it is rigorous, so we won't need to reprove the proposition after giving the formal definition of counting.

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 $\{a, a+1, a+2, \ldots, b\}$. In other words, there are exactly $b - a + 1$ integers between a and b (inclusive).

Note that the condition $a \leq b + 1$ ensures that $b - a + 1$ is not negative. Of course, if $a > b$, then the set $\{a, a+1, a+2, \ldots, b\}$ is empty, so it has 0 elements.

Convention 4.2.3. We agree to use the symbol "#" for "number".

4.3. Counting subsets

4.3.1. Counting them all

Now let us count something less trivial numbers.

Let us count the subsets of the set $\{1, 2, 3\}$. These are

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

There are 8 of them. More examples:

- There are 4 subsets of $\{1, 2\}$, namely $\{\}, \ \{1\}, \ \{2\}, \ \{1,2\}$.
- There are 2 subsets of $\{1\}$, namely $\{\}$ and $\{1\}$. (Note that any set A satisfies $\{\} \subseteq A$ and $A \subseteq A$.)
- There is 1 subset of $\{\}$, namely $\{\}$ itself.
- There are 16 subsets of $\{1, 2, 3, 4\}$.

At this point, the pattern should be clear:

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: The set $\{1, 2, \ldots, 0\}$ is empty, and thus has exactly 1 subset. This matches $2^0 = 1$. So the theorem holds for $n = 0$.

Induction step: We proceed from $n - 1$ to n. Thus, let n be a positive integer. Assume (as IH) that

$$(\#\text{ of subsets of } \{1, 2, \ldots, n-1\}) = 2^{n-1}.$$

Our goal is to prove that

$$(\#\text{ of subsets of } \{1, 2, \ldots, n\}) \overset{?}{=} 2^n.$$

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

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

whereas the green sets are

$$\{\}, \quad \{1\}, \quad \{2\}, \quad \{1,2\}.$$

Each subset of $\{1, 2, \ldots, n\}$ is either red or green, but not both. Hence,

$$\begin{aligned} &(\#\text{ of subsets of } \{1, 2, \ldots, n\}) \\ &= (\#\text{ of red sets}) + (\#\text{ of green sets}). \end{aligned}$$

So let us now count the red sets and the green sets separately.

We start with the green sets: These are the subsets of $\{1, 2, \ldots, n\}$ that do not contain n. In other words, they are just the subsets of $\{1, 2, \ldots, n-1\}$. Hence,

$$(\#\text{ of green sets}) = (\#\text{ of subsets of } \{1, 2, \ldots, n-1\}) = 2^{n-1}.$$

Let us now count the red sets. These are just the green sets, with an n inserted into them. More precisely: Each green set can be turned into a red set by inserting n into it. Conversely, each red set can be turned green by removing n from it. This way, each green set is paired up with a unique red set. Here is how this pairing looks like for $n = 3$:

$$\begin{array}{ccccc} \text{green} & \{\} & \{1\} & \{2\} & \{1,2\} \\ \text{red} & \{3\} & \{1,3\} & \{2,3\} & \{1,2,3\} \end{array}.$$

The existence of this pairing shows that

$$(\#\text{ of red sets}) = (\#\text{ of green sets}) = 2^{n-1}.$$

Altogether,

$$\begin{aligned}
&(\text{\# of subsets of } \{1,2,\ldots,n\}) \\
&= \underbrace{(\text{\# of red sets})}_{=2^{n-1}} + \underbrace{(\text{\# of green sets})}_{=2^{n-1}} \\
&= 2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n.
\end{aligned}$$

This completes the induction step. Thus, the theorem is proved. □

More generally:

Theorem 4.3.2. Let $n \in \mathbb{N}$. Let S be an n-element set. Then,

$$(\text{\# of subsets of } S) = 2^n.$$

Informal proof. Rename the n elements of S as $1, 2, \ldots, n$, and apply the previous theorem. □

For example,

$$(\text{\# of subsets of } \{\text{cat, dog, rat}\}) = 8.$$

4.3.2. Counting the subsets of a given size

Let us now refine our question: Instead of counting all subsets of $\{1, 2, \ldots, n\}$, we only count the k-element subsets of $\{1, 2, \ldots, n\}$ for a given number k.

For example, how many 2-element subsets does the set $\{1, 2, 3, 4\}$ have? These are

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

So there are 6 of them.

More generally:

Theorem 4.3.3. Let $n \in \mathbb{N}$, and let k be any number. 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

$$P(n) := \left(\begin{array}{c} \text{"for any number } k \text{ and any } n\text{-element set } S, \\ \text{we have } (\text{\# of } k\text{-element subsets of } S) = \dbinom{n}{k}\text{"} \end{array} \right)$$

for each $n \in \mathbb{N}$.

Base case: Let's prove $P(0)$. Let k be any number. The only 0-element set is $\varnothing$, and this set has only one subset, which is $\varnothing$ itself. Hence,

$$(\text{\# of } k\text{-element subsets of } \varnothing) = \begin{cases} 1, & \text{if } k = 0; \\ 0, & \text{else} \end{cases} = \binom{0}{k}.$$

So $P(0)$ is proved.

Induction step: Let n be a positive integer. Assume (as 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

$$(\text{\# of } k\text{-element subsets of } S) \overset{?}{=} \binom{n}{k}.$$

Again, we can rename the n elements of S as $1, 2, \ldots, n$. So we must prove that

$$(\text{\# of } k\text{-element subsets of } \{1, 2, \ldots, n\}) \overset{?}{=} \binom{n}{k}.$$

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 do not contain n.

Then, as before,

$$\begin{aligned} & (\text{\# of } k\text{-element subsets of } \{1, 2, \ldots, n\}) \\ & = (\text{\# of red sets}) + (\text{\# of green sets}). \end{aligned}$$

Let us now count the green sets. These are just the k-element subsets of $\{1, 2, \ldots, n-1\}$. Hence,

$$\begin{aligned} & (\text{\# of green sets}) \\ & = (\text{\# of } k\text{-element subsets of } \{1, 2, \ldots, n-1\}) \\ & = \binom{n-1}{k} \qquad (\text{by the IH}). \end{aligned}$$

Now to 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 the **blue sets**. Thus, if T is a red set, then $T \setminus \{n\}$ is a blue set. Conversely, if U is a blue set, then $U \cup \{n\}$ is a red set. This allows us to pair up each blue set with a red set and vice versa. Thus,

$$\begin{aligned}(\text{\# of red sets}) &= (\text{\# of blue sets}) \\ &= (\text{\# of } (k-1)\text{-element subsets of } \{1,2,\ldots,n-1\}) \\ &= \binom{n-1}{k-1} \qquad (\text{by the IH}).\end{aligned}$$

Altogether,

$$\begin{aligned}&(\text{\# of } k\text{-element subsets of } \{1,2,\ldots,n\}) \\ &= \underbrace{(\text{\# of red sets})}_{=\binom{n-1}{k-1}} + \underbrace{(\text{\# of green sets})}_{=\binom{n-1}{k}} \\ &= \binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k} \qquad (\text{by Pascal's recurrence}).\end{aligned}$$

This proves $P(n)$, and thus completes the induction. □

4.4. Tuples (aka lists)

4.4.1. Definition and disambiguation

Definition 4.4.1. A **finite list** (aka **tuple**) is a list consisting of finitely many objects. The objects appear in this list in a specified order, and they don't have to be distinct.

A finite list delimited using parentheses: i.e., the list that contains the objects $a_1, a_2, \ldots, a_n$ in this order is called $(a_1, a_2, \ldots, a_n)$.

"Specified order" means that the list has a well-defined first entry, a well-defined second 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 $n = m$;
- we have $a_i = b_i$ for each $i \in \{1, 2, \ldots, n\}$.

For example:

- The lists $(1, 2)$ and $(2, 1)$ are distinct, even though the sets $\{1, 2\}$ and $\{2, 1\}$ are equal.
- The lists $(1, 2)$ and $(1, 1, 2)$ are distinct, even though the sets $\{1, 2\}$ and $\{1, 1, 2\}$ are equal.

- The list $(1,1,2)$ and $(1,2,2)$ are distinct, even though the sets $\{1,1,2\}$ and $\{1,2,2\}$ are equal.

Definition 4.4.2. **(a)** The **length** of a list $(a_1, a_2, \ldots, a_n)$ is the number n.
(b) A list of length 2 is called a **pair** (or an **ordered 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 (though it has only 3 **distinct** entries), i.e., a quadruple or a 4-tuple. Meanwhile, $(5,8)$ is a 2-tuple, i.e., a pair.

There is only one list of length 0: the empty list $()$, which contains nothing.

Lists of length 1 consist of just a single entry: For any object o, there is a 1-tuple (o).

4.4.2. Counting pairs

Now let us count pairs (the simplest nontrivial lists):

- How many pairs (a,b) are there with $a,b \in \{1,2,3\}$? There are nine, namely
$$\begin{array}{ccc} (1,1), & (1,2), & (1,3), \\ (2,1), & (2,2), & (2,3), \\ (3,1), & (3,2), & (3,3). \end{array}$$
I have laid them out in a rectangular table, where each row determines the first entry of the pair (i.e., in the i-th row I've put all pairs starting with i), and each column determines the second entry. This table has 3 rows and 3 columns, thus $3 \cdot 3 = 9$ cells. So there are nine such pairs.

- How many pairs (a,b) are there with $a,b \in \{1,2,3\}$ and $a < b$? There are three, namely
$$(1,2), \qquad (1,3), \qquad (2,3).$$

- How many pairs (a,b) are there with $a,b \in \{1,2,3\}$ and $a = b$? There are three, namely
$$(1,1), \qquad (2,2), \qquad (3,3).$$

- How many pairs (a,b) are there with $a,b \in \{1,2,3\}$ and $a > b$? There are three, namely
$$(2,1), \qquad (3,1), \qquad (3,2).$$

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:

$$\begin{array}{cccc} (1,1), & (1,2), & \ldots, & (1,n), \\ (2,1), & (2,2), & \ldots, & (2,n), \\ \vdots & \vdots & \ddots & \vdots \\ (n,1), & (n,2), & \ldots, & (n,n) \end{array}$$

(where the rows determine the first entry and the columns determine the second). This table has $n \cdot n = n^2$ cells, so there are n^2 pairs.

(b) In the above table, the condition $a < b$ means that the pair (a, b) is above the main diagonal. So we need to count the cells of our table that are above the main diagonal. In the first column, there are 0 such cells. In the second column, there is 1. In the third, there are 2. And so on. In the last column, there are $n - 1$. So the total number of cells above the main diagonal is

$$0 + 1 + 2 + \cdots + (n-1) = 1 + 2 + \cdots + (n-1).$$

So there are $1 + 2 + \cdots + (n-1)$ many pairs (a, b) with $a < b$.

(c) We now need to count the cells on the main diagonal. In each column, there is exactly 1 of them. Altogether, there are therefore $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = n$ of them.

(d) The pairs (a, b) satisfying $a > b$ are in one-to-one correspondence with the pairs (a, b) satisfying $a < b$: 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 $1 + 2 + \cdots + (n-1)$ (by part **(b)**). Thus the # of former pairs is $1 + 2 + \cdots + (n-1)$. □

The proposition we just proved has a curious consequence: For any $n \in \mathbb{N}$, we have

$$\begin{aligned}
n^2 &= (\text{\# of pairs } (a,b) \text{ with } a,b \in \{1,2,\ldots,n\}) \\
&= (\text{\# of pairs } (a,b) \text{ with } a,b \in \{1,2,\ldots,n\} \text{ and } a<b) \\
&\qquad + (\text{\# of pairs } (a,b) \text{ with } a,b \in \{1,2,\ldots,n\} \text{ and } a=b) \\
&\qquad + (\text{\# of pairs } (a,b) \text{ with } a,b \in \{1,2,\ldots,n\} \text{ and } a>b) \\
&= \underbrace{(1+2+\cdots+(n-1))+n}_{=1+2+\cdots+n} + \underbrace{(1+2+\cdots+(n-1))}_{=(1+2+\cdots+n)-n} \\
&= (1+2+\cdots+n)+(1+2+\cdots+n)-n \\
&= 2\cdot(1+2+\cdots+n)-n.
\end{aligned}$$

Solving this for $1+2+\cdots+n$, we find

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

So we have reproved the Little Gauss formula by counting pairs.

Exercise 4.4.1. How many pairs (a,b) are there with $a \in \{1,2,3\}$ and $b \in \{1,2,3,4,5\}$?

Solution. By the same reasoning as in part **(a)** of the above proposition, we can arrange these pairs in a table with 3 rows and 5 columns. So there are $3\cdot 5 = 15$ of them. □

The same reasoning gives the following more general rule:

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, since

$$\begin{aligned}(\text{\# of elements of } U) &= (\text{\# of pairs } (a,b) \text{ with } a \in A \text{ and } b \in B)\\ &= nm \qquad\qquad (\text{by the previous theorem}).\end{aligned}$$

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 preceding theorem, since U is an nm-element set, and C is a p-element set). Since $(nm)\,p = nmp$, this is precisely what we need to prove. □

4.4.3. Cartesian products

There is a general notation 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** (or just **product**) of the sets A and B.

For instance, $\{1,2\} \times \{7,8,9\}$ is the set of all pairs (a,b) with $a \in \{1,2\}$ and $b \in \{7,8,9\}$. Explicitly, it consists of the six pairs

$$\begin{matrix}(1,7), & (1,8), & (1,9),\\ (2,7), & (2,8), & (2,9).\end{matrix}$$

A similar notation exists for k-tuples instead of pairs:

> **Definition 4.4.7.** Let $A_1, A_2, \ldots, A_k$ be k sets.
>
> 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 $A_1, A_2, \ldots, A_k$.

For instance, the set $\{1,2\} \times \{5\} \times \{2,7,6\}$ consists of all triples (a,b,c) with $a \in \{1,2\}$ and $b \in \{5\}$ and $c \in \{2,7,6\}$. Explicitly, these are the triples

$$\begin{array}{ccc} (1,5,2), & (1,5,7), & (1,5,6), \\ (2,5,2), & (2,5,7), & (2,5,6). \end{array}$$

The word "Cartesian" refers to René Descartes and his concept of Cartesian coordinates. In a Cartesian coordinate system, every point in space can be described by a triple of real numbers (its coordinates), so that space can be identified with the Cartesian product $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$. Similarly, the plane can be identified with $\mathbb{R} \times \mathbb{R}$.

Using Cartesian products, we can restate our above theorems as follows:

Theorem 4.4.8 (product rule for two sets)**.** If A is an n-element set, and B is an m-element set, then $A \times B$ is an nm-element set.

Theorem 4.4.9 (product rule for three sets)**.** If A is an n-element set, and B is an m-element set, and C is 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 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.

4.4.4. Counting strictly increasing tuples (informally)

Above we have shown that for any $n \in \mathbb{N}$, 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 $\{a,b,c\}$ of $\{1,2,\ldots,n\}$. Conversely, any 3-element subset of $\{1,2,\ldots,n\}$ becomes a triple (a,b,c) satisfying $a < b < c$ if you list its three 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 (i.e., there is a one-to-one correspondence between the former and the latter). Thus,

$$\begin{aligned}
&(\text{\# of triples } (a,b,c) \text{ of elements of } \{1,2,\ldots,n\} \text{ satisfying } a<b<c) \\
&= (\text{\# of 3-element subsets of } \{1,2,\ldots,n\}) \\
&= \binom{n}{3} \qquad \text{(by a theorem from the previous section)}.
\end{aligned}$$

More generally, for any $k \in \mathbb{N}$, we have

$$\begin{aligned}
&(\text{\# of } k\text{-tuples } (a_1,a_2,\ldots,a_k) \text{ of elements of } \{1,2,\ldots,n\} \text{ satisfying } a_1<a_2<\cdots<a_n) \\
&= \binom{n}{k}
\end{aligned}$$

(by the same argument). For comparison,

$$\begin{aligned}
&(\text{\# of } k\text{-tuples } (a_1,a_2,\ldots,a_k) \text{ of elements of } \{1,2,\ldots,n\}) \\
&= \underbrace{nn\cdots n}_{k\text{ times}} \qquad \text{(by the product rule for } k \text{ sets)} \\
&= n^k.
\end{aligned}$$

Not every counting problem has such a nice answer. For instance, it is not hard to check that

$$\begin{aligned}
&(\text{\# of } k\text{-tuples } (a_1,a_2,\ldots,a_k) \text{ of elements of } \{1,2,\ldots,n\} \text{ with largest entry } a_1) \\
&= 1^{k-1}+2^{k-1}+\cdots+n^{k-1},
\end{aligned}$$

but there is no closed form for the RHS without $\sum$ signs or "$\cdots$"s.

In the next two chapters, we will put the notion of counting on a rigorous footing. For this purpose, we must get familiar with the concept of **maps** (aka **functions**).

5.

6. Maps (aka functions)

6.1. Functions, informally

One of the main notions in mathematics 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 6.1.1** (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.

This is not a real definition, since it just kicks the can down the road: What is a "rule"? But it gives the right intuition, as long as you understand it correctly. Here are some clarifying comments:

- A function has to "work" for each element of X. It cannot decline to operate on some elements. For example, "take the reciprocal" is not a function from $\mathbb{R}$ to $\mathbb{R}$, since it would not operate on 0 (since 0 has no reciprocal).

- 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 $\mathbb{R}$, since different powers give different results.

- The result of applying a function f to an input x is denoted by $f(x)$ or sometimes by fx.

- 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 takes 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 "$f : x \mapsto y$".

  For instance, if f is the "take the square" function from $\mathbb{R}$ to $\mathbb{R}$, then $f : 2 \mapsto 4$ and f takes 2 to 4 and f transforms 2 into 4, etc.

- As the above terminology suggests, the **value** of a function f at an input x means the corresponding output $f(x)$.

- When are two functions equal? In programming, functions are often understood to be (implemented) algorithms, and two algorithms can differ even if they compute the same thing. In mathematics, on the other hand, the outputs are what matters, not the implementation (and in fact, there might even not be any implementation).

  So when are two functions considered 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

$$X_1 = X_2 \qquad \text{and} \qquad Y_1 = Y_2 \qquad \text{and}$$
$$f_1(x) = f_2(x) \qquad \text{for all } x \in X_1.$$

An example of two equal functions is:

- the function $f_1 : \mathbb{R} \to \mathbb{R}$ that sends each x to x^2;
- the function $f_2 : \mathbb{R} \to \mathbb{R}$ that sends each x to $|x|^2$,

since each $x \in \mathbb{R}$ satisfies $x^2 = |x|^2$.

- Let $f : Y \to Z$ and $g : X \to Y$ be two functions. Then, $f \circ g$ (pronounced "f **after** g" or "the **composition** of f and g") denotes the function from X to Z that sends each $x \in X$ to $f(g(x))$. In other words, it satisfies

$$(f \circ g)(x) = f(g(x)) \qquad \text{for each } x \in X.$$

For example, if $f : \mathbb{R} \to \mathbb{R}$ is the sin function and if $g : \mathbb{R} \to \mathbb{R}$ is the "take the square" function, then $f \circ g$ is the function that takes each $x \in \mathbb{R}$ to $\sin(x^2)$. In contrast, $g \circ f$ is the function that takes each $x \in \mathbb{R}$ to $(\sin x)^2$. This shows that even when $f \circ g$ and $g \circ f$ are both defined, they don't have to be the same.

- The notation

$$X \to Y,$$
$$x \mapsto (\text{some expression involving } x)$$

means "the function from X to Y that sends each element x of X to the expression on the right hand side". Here, the expression can be (for example) x^2 or $\frac{1}{x+4}$ or $\frac{x}{x+2}$ or $(\sin x)^{15}$.

For example,

$$\mathbb{R} \to \mathbb{R},$$
$$x \mapsto x^2$$

is the "take the square" function (sending each element x of $\mathbb{R}$ to x^2). For another example,

$$\mathbb{R} \to \mathbb{R},$$
$$x \mapsto \frac{x}{\sin x + 13}$$

is the function that takes the sine of the input, then adds 13, and then divides the input by the result.

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; this is an example of a constant function.

For yet another example,

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Q}, \\ x &\mapsto 2^x \end{aligned}$$

is a function. Some of its values are

x	-2	-1	0	1	2
2^x	$\frac{1}{4}$	$\frac{1}{2}$	1	2	4

.

- The notation

$$\begin{aligned} f : X &\to Y, \\ x &\mapsto \text{(some expression involving } x\text{)} \end{aligned}$$

means that we take the function from X to Y that sends each $x \in X$ to the expression on the RHS, 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 will henceforth 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 by simply listing all its values. For example, we can define a function $h : \{1, 5, 8\} \to \mathbb{Z}$ by setting

$$h(1) = 30, \qquad h(5) = 18, \qquad h(8) = 30.$$

The values here have been chosen at whim; they don't need to follow any rule or pattern.

- If f is a function from X to Y, then the sets X and Y are part of the function. Thus,

  $$\begin{aligned} g_1 : \mathbb{Z} &\to \mathbb{Q}, \\ x &\mapsto 2^x \end{aligned}$$

  and

  $$\begin{aligned} g_2 : \mathbb{N} &\to \mathbb{Q}, \\ x &\mapsto 2^x \end{aligned}$$

  and

  $$\begin{aligned} g_3 : \mathbb{N} &\to \mathbb{N}, \\ x &\mapsto 2^x \end{aligned}$$

  are three distinct functions! We distinguish between them in order to have well-defined notions of "domain" and "target". Namely, the **domain** of a function $f : X \to Y$ is defined to be the set X, whereas the **target** of this map is defined to be the set Y. For example, g_1 and g_2 have different domains (g_1 has domain $\mathbb{Z}$ while g_2 has domain $\mathbb{N}$), whereas g_2 and g_3 have different targets (g_2 has target $\mathbb{Q}$ while g_3 has target $\mathbb{N}$).

At this point, we have an idea what a function is, but the provisional definition we gave above is not fully precise. In particular, when a function is not given by an explicit formula or specified by a finite list of values, we might get into doubts about whether it is a function. Thus we eventually need a rigorous definition of a function.

This we shall give in a moment. We will define functions to be relations with a certain property. So let us define relations first.

6.2. Relations

Relations (to be specific: binary relations) are another concept whose many examples you are already familiar with:

- The relation $\subseteq$ is a relation between two sets. For example, $\{2,4\} \subseteq \{1,2,3,4\}$ but $\{2,5\} \not\subseteq \{1,2,3,4\}$.

- The order relations $\leq$ and $<$ and $>$ and $\geq$ are relations between two integers (or rational numbers or real numbers). For example, $1 \leq 1$ and $1 \leq 5$ and $1 \not\leq 0$.

- The containment relation $\in$ is a relation between an object and a set. For instance, $3 \in \{1,2,3\}$ but $5 \notin \{1,2,3\}$.

- The divisibility relation $|$ is a relation between two integers.
- The relation "coprime" is a relation between two integers.
- Plane geometry is a great source of relations: "parallel" (a relation between lines), "perpendicular", "congruent" (a relation between shapes), "similar", "directly similar", ...
- For any given integer n, the relation "congruent modulo n" is a relation between two integers. Let me call it $\overset{n}{\equiv}$. Thus, $a \overset{n}{\equiv} b$ means $a \equiv b \bmod n$. For example, $2 \overset{3}{\equiv} 8$ but $2 \overset{3}{\not\equiv} 7$.

What do all these relations have in common? They can be applied to pairs of objects. Applying a relation to a pair of objects gives a statement which is either true or false. For example, applying the relation "coprime" to the pair $(5, 8)$ yields the statement "5 is coprime to 8", which is true. But applying it to the pair $(5, 10)$ yields the statement "5 is coprime to 10", which is false.

A general relation R relates elements of a set X with elements of a set Y. For any pair $(x, y) \in X \times Y$, we can apply the relation R to the 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 $(x, y) \in X \times Y$ 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 of a relation, we simply define the relation R to be this set:

Definition 6.2.1. Let X and Y be two sets. A **relation** from X to Y is a subset of $X \times Y$.

If R is a relation from X to Y, and if $(x, y) \in X \times Y$ is a 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

$$\begin{aligned} &\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \ | \ x \text{ divides } y\} \\ &= \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \ | \ \text{there exists some } z \in \mathbb{Z} \text{ such that } y = xz\} \\ &= \{(x, xz) \ | \ x \in \mathbb{Z} \text{ and } z \in \mathbb{Z}\}. \end{aligned}$$

For instance, the pairs $(2, 4)$ and $(3, 12)$ and $(10, 20)$ belong to this subset, but the pairs $(2, 3)$ and $(12, 3)$ and $(10, 5)$ do not.

- The coprimality relation ("coprime to") 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 any $n \in \mathbb{Z}$, the "congruent modulo n" relation $\overset{n}{\equiv}$ is a subset of $\mathbb{Z} \times \mathbb{Z}$, namely the subset

$$\begin{aligned} &\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \equiv y \bmod n\} \\ &= \{(x,\ x + nz) \mid x \in \mathbb{Z} \text{ and } z \in \mathbb{Z}\}. \end{aligned}$$

- A geometric example: Let P be the set of all points in the plane, and let L be the set of all lines in the plane. Then, the "lies on" relation (as in "a point lies on a line") is a subset of $P \times L$, namely the subset

$$\{(p,\ell) \in P \times L \mid p \text{ lies on } \ell\}.$$

- 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 and y satisfy $x \ E_A \ y$ if and only if they are equal.

- We can literally take any subset of $X \times Y$ and it will be a relation from X to Y. It does not have to be defined by a "meaningful" rule. For example, here is a relation from $\{1,2,3\}$ to $\{5,6,7\}$:

$$\{(1,6),\ (1,7),\ (3,5)\}.$$

  Equivalently, it can be described by its truth table:

	5	6	7
1	no	yes	yes
2	no	no	no
3	yes	no	no

  (where a "yes" in row x and column y means that (x,y) belongs to the relation). If we call this relation R, then we have $1 \ R \ 6$ and $1 \ R \ 7$ and $3 \ R \ 5$ but $1 \not R \ 5$ and $2 \not R \ 6$.

A good way to visualize a relation R from a set X to a set Y is to draw a node for each element of X and a node for each element of Y, and to draw an arrow from the x-node to the y-node for every pair $(x,y) \in R$.

6.3. Functions, formally

We can now define functions properly:

> **Definition 6.3.1** (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 that has the following property:
>
> > **Output uniqueness:** For each $x \in X$, there exists **exactly one** $y \in Y$ such that $x\ R\ y$.
>
> If R is a function from X to Y, and if $x \in X$, then the unique element $y \in Y$ satisfying $x\ R\ y$ will be called $R(x)$.

In our above example, the relation

$$\{(1,6),\ (1,7),\ (3,5)\}$$

is not a function from $\{1,2,3\}$ to $\{5,6,7\}$, since it fails output uniqueness for $x = 1$ and also fails it for $x = 2$. Either failure would be enough to disqualify it.

Among all our above examples of relations, only the equality relation E_A is a function.

Another example of a function is the relation

$$\{(1,2),\ (2,1),\ (3,1)\}$$

from $\{1,2,3\}$ to $\{1,2,3\}$. This relation satisfies output uniqueness, so it is a function. If we call it f, then $f(1) = 2$ and $f(2) = 1$ and $f(3) = 1$.

In terms of our blobs-and-arrows picture, output uniqueness simply says that each x-node (for each $x \in X$) is the starting point of exactly one arrow.

We now have two definitions of functions: the provisional one (as "rules" that transforms inputs into outputs) and the rigorous one (as relations that satisfy output uniqueness). These definitions are equivalent, since:

- If R is a rigorous function from X to Y, then we can view R as a provisional function, which sends each $x \in X$ to the unique $y \in Y$ that satisfies $x\ R\ y$.
- Conversely: If f is a privisional function from X to Y, then the corresponding rigorous function is the relation

  $$\{(x,\ f(x))\ \mid\ x \in X\}.$$

  In other words, this is the relation that relates each input to its corresponding output under f.

6.4. Some more examples of functions

Example 6.4.1. 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

$$\{(1,3), \ (2,2), \ (3,3), \ (4,3)\}.$$

Example 6.4.2. What about the function

$$\begin{aligned} f_1 : \{1,2,3,4\} &\to \{1,2,3\}, \\ n &\mapsto n \ ? \end{aligned}$$

Such a function f_1 does not exist, since it would have to send 4 to 4, but 4 is not in the target $\{1,2,3\}$.

The problem here is that not every expression that appears to define a function actually defines a function. Make sure that the expression to the right of "$\mapsto$" always is an actual element of the target.

Example 6.4.3. Consider the function

$$\begin{aligned} f_2 : \{1,2,3,\ldots\} &\to \{1,2,3,\ldots\}, \\ n &\mapsto (\text{the number of positive divisors of } n). \end{aligned}$$

As a relation, it is

$$\{(1,1), \ (2,2), \ (3,2), \ (4,3), \ (5,2), \ (6,4), \ (7,2), \ (8,4), \ (9,3), \ \ldots\}.$$

Thus, $f_2(1) = 1$ and $f_2(2) = 2$ and $f_2(3) = 2$ and so on.

Example 6.4.4. What about the function

$$\begin{aligned} \widetilde{f_2} : \mathbb{Z} &\to \{1,2,3,\ldots\}, \\ n &\mapsto (\text{the number of positive divisors of } n) \ ? \end{aligned}$$

Again, there is no such function $\widetilde{f_2}$, since $\widetilde{f_2}(0)$ would have to be ∞ or undefined (every integer divides 0), which in either case is not an element of the target $\{1,2,3,\ldots\}$.

Example 6.4.5. What about the function

$$\begin{aligned} f_3 : \{1,2,3,\ldots\} &\to \{1,2,3,\ldots\}, \\ n &\mapsto (\text{the smallest prime divisor of } n) \ ? \end{aligned}$$

Again, there is no such function f_3, since $f_3(1)$ is undefined (1 has no prime divisors).

However, we can salvage f_3: Either we make it a relation

$$\{(n,\ p) \mid p \text{ is the smallest prime divisor of } n\},$$

or we restrict it to $\{2,3,4,\ldots\}$. The restricted version

$$\begin{aligned} \widetilde{f_3} : \{2,3,4,\ldots\} &\to \{1,2,3,\ldots\}, \\ n &\mapsto (\text{the smallest prime divisor of } n) \end{aligned}$$

is a function.

Example 6.4.6. What about the function

$$\begin{aligned} f_4 : \mathbb{Q} &\to \mathbb{Z}, \\ \frac{a}{b} &\mapsto a \qquad (\text{for } a, b \in \mathbb{Z} \text{ with } b \neq 0) \ ? \end{aligned}$$

Restated in 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?

Again, the answer is **no**. The problem is again a failure of output uniqueness, but this time because there are too many different outputs for a given input. For example, $f_4\left(\frac{1}{1}\right)$ would be 1 but $f_4\left(\frac{2}{2}\right)$ would be 2. However, $\frac{1}{1} = \frac{2}{2}$, so that $f_4\left(\frac{1}{1}\right)$ should equal $f_4\left(\frac{2}{2}\right)$. This is a contradiction.

The underyling issue is that a rational number can be written as a fraction in several different ways, and the numerators of these fractions will be different. Thus, the rule $\frac{a}{b} \mapsto a$ will produce different outputs from the same input.

6.5. Well-definedness

We have seen several ways in which the definition of a function can go wrong. Situations where they don't go wrong are called "**well-definedness**". Thus we say that "a function is well-defined" to mean that "our definition does not suffer from the above issues". So you should read "This function is well-defined [resp. not well-defined]" as "The definition we just gave actually defines a function [resp. does not define a function]".

For example, as we just saw, the function

$$\begin{aligned} f_4 : \mathbb{Q} &\to \mathbb{Z}, \\ \frac{a}{b} &\mapsto a \end{aligned}$$

is not well-defined (i.e., there is no such function), but the function

$$\begin{aligned} f_5 : \mathbb{Q} &\to \mathbb{Q}, \\ \frac{a}{b} &\mapsto \frac{a^2}{b^2} \end{aligned}$$

is well-defined (in fact, it can be rewritten without reference to a specific fraction, as $x \mapsto x^2$). For another example, the function

$$\begin{aligned} f_1 : \{1,2,3,4\} &\to \{1,2,3\}, \\ n &\mapsto n \end{aligned}$$

is not well-defined (since its supposed output $f_1(4)$ does not lie in the target), whereas the function

$$\begin{aligned} f_6 : \{1,2,3,4\} &\to \{1,2,3\}, \\ n &\mapsto 1 + (n\%3) \end{aligned}$$

is well-defined (since its values do lie in the target).

6.6. The identity function

Definition 6.6.1. For any set A, there is an **identity function** $\mathrm{id}_A : A \to A$. This is the function that sends each element $a \in A$ to a itself. It is precisely the relation E_A we defined above.

6.7. More examples, and multivariate functions

As we said before, a function $f : X \to Y$ can be described either by a rule or by a list of values (if X is finite) or as a relation. For instance, the "take the square" function on real numbers is the function

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto x^2. \end{aligned}$$

As a relation, it is the set

$$\left\{ \left(x, x^2\right) \mid x \in \mathbb{R} \right\}.$$

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

$$f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \\ (a, b) \mapsto a + b$$

(which sends each pair (a, b) of two integers to their sum $a + b$) is a multivariate function. Its input is a pair of two integers, i.e., it really has two inputs (a and b). As a relation, it is the subset

$$\{((a, b)\ ,\ a + b)\ \mid\ a, b \in \mathbb{Z}\} \\ = \{((a, b)\ ,\ c)\ \mid\ a, b, c \in \mathbb{Z} \text{ and } c = a + b\}$$

of $(\mathbb{Z} \times \mathbb{Z}) \times \mathbb{Z}$. Of course, this function has a name: addition of integers. Other multivariate functions are

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \\ (a, b) \mapsto a - b$$

and

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \\ (a, b) \mapsto ab$$

as well as analogous functions defined for other types of numbers. However, there is no "division" function

$$\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \\ (a, b) \mapsto a/b$$

(but there is a division function

$$\mathbb{Q} \times (\mathbb{Q} \setminus \{0\}) \to \mathbb{Q}, \\ (a, b) \mapsto a/b$$

).

When f is a multivariate function whose inputs are k-tuples, we commonly use the notation

$$f(a_1, a_2, \ldots, a_k) \qquad \text{for} \qquad f((a_1, a_2, \ldots, a_k)).$$

For example, if f is the addition of integers, then $f(a, b) = f((a, b)) = a + b$ for all $a, b \in \mathbb{Z}$.

6.8. Composition of functions

6.8.1. Definition

Recall how functions are composed:

Definition 6.8.1. Let X, Y, 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 the functions f and g, and is pronounced "f after g".

In terms of relations, if we view f and g as two relations F and G (as in our rigorous definition of a function), then $f \circ g$ is the relation

$$\left\{(x, z) \mid \text{there exists } y \in Y \text{ such that } x\ G\ y \text{ and } y\ F\ z\right\}.$$

Example 6.8.2. Consider the two functions

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto x^3 \end{aligned}$$

and

$$\begin{aligned} g : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto \frac{1}{x^2 + 7}. \end{aligned}$$

Then, for any $x \in \mathbb{R}$, we have

$$\left(f \circ g\right)\left(x\right) = f\left(g\left(x\right)\right) = f\left(\frac{1}{x^2+7}\right) = \left(\frac{1}{x^2+7}\right)^3$$

and

$$\left(g \circ f\right)\left(x\right) = g\left(f\left(x\right)\right) = g\left(x^3\right) = \frac{1}{\left(x^3\right)^2 + 7} = \frac{1}{x^6+7}.$$

These two results are different; thus, $f \circ g \neq g \circ f$.

6.8.2. Basic properties

Here are two basic facts that are proved in the notes:

Theorem 6.8.3 (associativity of composition)**.** We have

$$\left(f \circ g\right) \circ h = f \circ \left(g \circ h\right)$$

whenever the compositions make sense (i.e., whenever X, Y, Z, W are four sets and $f : Z \to W$ and $g : Y \to Z$ and $h : X \to Y$ are three maps).

> **Theorem 6.8.4.** Let $f : X \to Y$ be a map. Then,
>
> $$f \circ \operatorname{id}_X = \operatorname{id}_Y \circ f = f.$$

6.9. Jectivities (injectivity, surjectivity, bijectivity)

Now we define some important properties of functions.

> **Definition 6.9.1.** 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: 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: f is **surjective** if every element of Y is an output 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 $f(x) = y$.
>
> In other words: f is **bijective** if f is both injective and surjective.

Some examples:

- The function

  $$f : \mathbb{N} \to \mathbb{N},$$
  $$k \mapsto k^2$$

  is injective (since no two different nonnegative integers have the same square) but not surjective (since not every nonnegative integer is a perfect square – e.g., the integer 3 is not). So it is not bijective.

- Let $S = \{0, 1, 4, 9, 16, 25, \ldots\}$ be the set of all perfect squares (= squares of integers = squares of nonnegative integers). Then, the function

  $$g : \mathbb{N} \to S,$$
  $$k \mapsto k^2$$

  is injective (for the same reason as f) and is surjective (since every $s \in S$ is a value of g), so it is bijective.

- The function

  $$\begin{aligned} g_{\text{int}} : \mathbb{Z} &\to S, \\ k &\mapsto k^2 \end{aligned}$$

  is still surjective, but not injective (since $g_{\text{int}}(-1) = g_{\text{int}}(1)$), so it again fails to be bijective.

- The function

  $$\begin{aligned} h : \mathbb{N} &\to \mathbb{N}, \\ k &\mapsto k//2 \end{aligned}$$

  is not injective (since $h(4) = h(5)$), but is surjective (since each $n \in \mathbb{N}$ equals $h(2n)$). It is again not bijective.

- Let $E = \{0, 2, 4, 6, \ldots\}$ be the set of all even nonnegative integers. Then, the function

  $$\begin{aligned} h_{\text{even}} : E &\to \mathbb{N}, \\ k &\mapsto k//2 \end{aligned}$$

  is injective (since $k//2 = k/2$ for each $k \in E$) and surjective (since each $n \in \mathbb{N}$ equals $h_{\text{even}}(2n)$). So it is bijective.

- Let $O = \{1, 3, 5, 7, 9, \ldots\}$ be the set of all odd nonnegative integers. Then, the function

  $$\begin{aligned} h_{\text{odd}} : O &\to \mathbb{N}, \\ k &\mapsto k//2 \end{aligned}$$

  is injective (since $k//2 = (k-1)/2$ for each $k \in O$) and surjective (since each $n \in \mathbb{N}$ equals $h_{\text{odd}}(2n+1)$). So it is bijective.

- Consider the map

  $$\begin{aligned} f : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}, \\ (a, b) &\mapsto a + b \end{aligned}$$

  (the addition of integers). This map f is not injective (since $f(3,4) = f(5,2)$ or since $f(1,0) = f(0,1)$), but is surjective (since $n \in \mathbb{Z}$ is $f(0,n)$).

Remark 6.9.2. Consider a function $f : X \to Y$ given by a table of all its values (possibly an infinite table if X is infinite). Assume that all possible inputs $x \in X$ appear on the top row of the table (each exactly once), and the corresponding outputs appear under them in the bottom row, so the table looks as follows:

x	a	b	c	$\cdots$
$f(x)$	$f(a)$	$f(b)$	$f(c)$	$\cdots$

.

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 each $y \in Y$ appears on the bottom row of the table.

(c) The function f is bijective if and only if each $y \in Y$ appears exactly once on the bottom row.

For example, the map $f : \{1, 2, 3\} \to \{1, 4\}$ with value table

x	1	2	3
$f(x)$	4	1	4

is not injective (since there are two 4's on the bottom row) but is surjective (since all elements of $\{1, 4\}$ appear on the bottom row).

We can also restate the definition of (in/sur/bi)jectivity in terms of the blobs-and-arrows picture: If a map $f : X \to Y$ is visualized as such a picture, then

- f is injective if and only if no two arrows hit the same Y-node.
- f is surjective if and only if each Y-node is hit by at least one arrow.
- f is bijective if and only if each Y-node is hit by exactly one arrow.

6.10. Inverses

Bijective maps have a special power: they can be **inverted**. Let us define what this means:

Definition 6.10.1. 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

$$\begin{aligned} f(g(y)) &= y && \text{for each } y \in Y, && \text{and} \\ g(f(x)) &= x && \text{for each } x \in X. \end{aligned}$$

Roughly speaking, an inverse of f thus means a map that undoes f and is undone by f.

Not every function has an inverse. We shall soon see which ones do. First, some examples:

- Let $f : \{1,2,3\} \to \{5,6,7\}$ be the "add 4" map, i.e., the map

  $$\begin{aligned} \{1,2,3\} &\to \{5,6,7\}, \\ k &\mapsto k+4. \end{aligned}$$

  This map f has an inverse: the "subtract 4" map

  $$\begin{aligned} g : \{5,6,7\} &\to \{1,2,3\}, \\ k &\mapsto k-4. \end{aligned}$$

  To see that g is an inverse of f, we must prove that each $y \in \{5,6,7\}$ satisfies $f(g(y)) = y$, and that each $x \in \{1,2,3\}$ satisfies $g(f(x)) = x$. This is easy: For each $y \in \{5,6,7\}$, we have

  $$f(g(y)) = (y-4)+4 = y.$$

  Similarly for the other equation.

- Let $f : \{1,2,3,4,5\} \to \{1,2,3,4,5\}$ be the map with the value table

x	1	2	3	4	5
$f(x)$	3	4	1	5	2

  .

  This map f has an inverse, namely the map $g : \{1,2,3,4,5\} \to \{1,2,3,4,5\}$ given by

y	1	2	3	4	5
$g(y)$	3	5	1	2	4

  .

- Let $f : \{1,2,3,4\} \to \{1,2,3,4\}$ be the function with the value table

x	1	2	3	4
$f(x)$	1	2	3	3

  .

  This function f has no inverse, since any inverse g of f would have to satisfy both $g(3) = 3$ and $g(3) = 4$, which is a contradiction. The underlying issue here is that f is not injective, so there are two different inputs giving the same output, and the inverse g would have to send that output to both of these inputs at once.

- Let $f : \{1, 2, 3\} \to \{1, 2, 3, 4\}$ be the function with the value table

x	1	2	3
$f(x)$	1	2	3

  .

  This function f has no inverse, because if g was an inverse of f, then $g(4)$ would have to be an $x \in \{1, 2, 3\}$ that f sends to 4, but there is no such x. The underlying issue here is that f is not surjective, so some $y \in Y$ is not hit by any arrow, and thus the inverse g does not have any element of x to send it to.

6.10.1. Invertibility is bijectivity by another name

Combining the two last examples, we see that only bijective maps have a chance at having an inverse. It is not hard to see that this is actually necessary and sufficient: Any bijective map has an inverse. We summarize:

> **Theorem 6.10.2.** 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. The "only if" part has been argued in the above two examples.

For the "if" part, let us assume that f is bijective. Now, define $g : Y \to X$ to be the map that sends each $y \in Y$ to the unique $x \in X$ that satisfies $f(x) = y$. It is easy to see that this g is an inverse of f, so f has an inverse. (See the notes for details.) □

6.10.2. Uniqueness of the inverse

> **Theorem 6.10.3.** Let $f : X \to Y$ be a function. Then, f has at most one inverse.

Proof. In other words, we must show that any two inverses of f must be equal. See the notes for that (Theorem 5.10.3). □

> **Definition 6.10.4.** Let $f : X \to Y$ be a function that has an inverse. Then, we call this inverse "**the inverse of** f" (since the theorem above shows that it is unique), and we denote it by f^{-1}.

Thus, if $f : X \to Y$ is a map that has an inverse, then we have

$$f^{-1} \circ f = \mathrm{id}_X \qquad \text{and} \qquad f \circ f^{-1} = \mathrm{id}_Y,$$

that is,

$$\begin{aligned} f^{-1}(f(x)) &= x \qquad \text{for all } x \in X, \qquad \text{andm} \\ f\left(f^{-1}(y)\right) &= y \qquad \text{for all } y \in Y. \end{aligned}$$

6.10.3. More examples

- Let $E = \{0, 2, 4, 6, \ldots\}$ be the set of all even nonnegative integers. Then, the function
  $$\begin{aligned} f : E &\to \mathbb{N}, \\ k &\mapsto k//2 = k/2 \end{aligned}$$
  has an inverse. This inverse is the function
  $$\begin{aligned} f^{-1} : \mathbb{N} &\to E, \\ k &\mapsto 2k. \end{aligned}$$
- Let $\mathbb{R}_{\geq 0} = \{\text{all nonnegative real numbers}\}$. Then, the function
  $$\begin{aligned} f : \mathbb{R}_{\geq 0} &\to \mathbb{R}_{\geq 0}, \\ x &\mapsto x^2 \end{aligned}$$
  has an inverse. This inverse is the function
  $$\begin{aligned} f^{-1} : \mathbb{R}_{\geq 0} &\to \mathbb{R}_{\geq 0}, \\ x &\mapsto \sqrt{x}. \end{aligned}$$
- In contrast, the function
  $$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto x^2 \end{aligned}$$
  has no inverse (as it is neither injective nor surjective, so definitely not bijective). But the function
  $$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto x^3 \end{aligned}$$
  has an inverse, which is the function
  $$\begin{aligned} f^{-1} : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto \sqrt[3]{x}. \end{aligned}$$

6.10.4. Inverses of inverses and compositions

Here are a few basic properties of inverses (see the notes for proofs):

Proposition 6.10.5. Let X be any set. Then, the identity map $\operatorname{id}_X : X \to X$ has an inverse, namely itself.

Theorem 6.10.6. Let $f : X \to Y$ be a map that has an inverse $f^{-1} : Y \to X$. Then, f^{-1} has an inverse, which is f.

Theorem 6.10.7 (socks-and-shoes formula)**.** Let X, Y, Z be three sets, and let $f : Y \to Z$ and $g : X \to Y$ be two bijective maps. Then, $f \circ g : X \to Z$ is again bijective, and its inverse is

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}.$$

Notice that the RHS here is $g^{-1} \circ f^{-1}$, not $f^{-1} \circ g^{-1}$.

Remark 6.10.8. The socks-and-shoes formula shows that the composition of two bijective maps is always bijective. However, a composition of two non-bijective maps can sometimes also be bijective.

See the notes (§5.11) for some solved exercises.

6.11. Isomorphic sets

Definition 6.11.1. Let X and Y be two sets. Then, we say that these two sets X and Y are **isomorphic as sets** (or, for short, **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 so are Y and X.

Some examples:

- The sets $\{1, 2, 3\}$ and $\{5, 6, 7\}$ are isomorphic, since there is a bijection from $\{1, 2, 3\}$ to $\{5, 6, 7\}$ (namely, for example, the "add 4" map).
- The sets $\{1, 2, 3\}$ and $\{1, 2\}$ are not isomorphic, since any bijective map from $\{1, 2, 3\}$ to $\{1, 2\}$ would have to use 3 arrows, but this would force it to hit some element of $\{1, 2\}$ at least twice.
- The sets $\{1, 2, 3\}$ and $\{1, 6, 75\}$ are isomorphic, since the map $f : \{1, 2, 3\} \to \{1, 6, 75\}$ with value table

x	1	2	3
$f(x)$	1	6	75

  is a bijection.

- The sets $\mathbb{N}$ and $E := \{\text{all even nonnegative integers}\}$ are isomorphic, since the map

  $$\mathbb{N} \to E, \\ n \mapsto 2n$$

  is a bijection.

- The sets $\mathbb{N}$ and $O := \{\text{all odd nonnegative integers}\}$ are isomorphic, since the map

  $$\mathbb{N} \to O, \\ n \mapsto 2n+1$$

  is a bijection.

- The sets $\mathbb{N}$ and $\mathbb{Z}$ are isomorphic, since there is a bijection from $\mathbb{N}$ to $\mathbb{Z}$ that sends

  $$\begin{array}{ll} 0,1,2,3,4,5,6,7,\ldots & \text{to} \\ 0,1,-1,2,-2,3,-3,4,-4,\ldots, & \text{respectively.} \end{array}$$

  Explicitly, this f can be defined by the formula

  $$f(n) = \begin{cases} -n/2, & \text{if } n \text{ is even;} \\ (n+1)/2, & \text{if } n \text{ is odd.} \end{cases}$$

- The sets $\mathbb{N}$ and $\mathbb{Q}$ are isomorphic, since there is a bijection from $\mathbb{N}$ to $\mathbb{Q}$ that sends

  $0,1,2,3,4,5,6,7,\ldots$ to

  $$\underbrace{\frac{-1}{1}, \frac{0}{1}, \frac{1}{1}}_{\substack{\text{all reduced fractions} \\ \text{whose numerator} \\ \text{and denominator are } \leq 1 \\ \text{in absolute value} \\ \text{(ordered from smallest} \\ \text{to largest)}}}, \quad \underbrace{\frac{-2}{1}, \frac{-1}{2}, \frac{1}{2}, \frac{2}{1}}_{\substack{\text{all reduced fractions} \\ \text{whose numerator} \\ \text{and denominator are } \leq 2 \\ \text{in absolute value} \\ \text{(ordered from smallest} \\ \text{to largest)}}}, \quad \underbrace{\frac{-3}{1}, \frac{-3}{2}, \frac{-2}{3}, \frac{-1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{3}{2}, \frac{3}{1}}_{\substack{\text{all reduced fractions} \\ \text{whose numerator} \\ \text{and denominator are } \leq 3 \\ \text{in absolute value} \\ \text{(ordered from smallest} \\ \text{to largest)}}}, \quad \ldots.$$

- The sets $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$ are isomorphic, since there is a bijection f from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$ that sends

  $0,1,2,3,4,5,\ldots$ to

  $$\underbrace{(0,0)}_{\substack{\text{all pairs} \\ \text{whose entries} \\ \text{sum to } 0}}, \quad \underbrace{(1,0), (0,1)}_{\substack{\text{all pairs} \\ \text{whose entries} \\ \text{sum to } 1 \\ \text{(ordered by} \\ \text{increasing 2nd} \\ \text{entry)}}}, \quad \underbrace{(2,0), (1,1), (0,2)}_{\substack{\text{all pairs} \\ \text{whose entries} \\ \text{sum to } 2 \\ \text{(ordered by} \\ \text{increasing 2nd} \\ \text{entry)}}}, \quad \ldots.$$

The inverse $f^{-1} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ of this bijection can be described by an explicit formula:

$$f^{-1}(n, m) = \frac{(n+m)(n+m+1)}{2} + m$$

(nice exercise: why?).

- The sets $\mathbb{N}$ and $\mathbb{R}$ are **not** isomorphic. See the notes for references to proofs of this (or google Cantor's diagonal argument).

7. Enumeration revisited

7.1. Counting, formally

7.1.1. Definition

As you have probably noticed, isomorphic sets have the same size (= number of elements). We shall now use this to **define** the size of a set!

First, some notations:

Definition 7.1.1. **(a)** If $n \in \mathbb{N}$, then $[n]$ shall mean the set $\{1, 2, \ldots, n\}$.

For example, $[3] = \{1, 2, 3\}$ and $[7] = \{1, 2, \ldots, 7\}$ and $[0] = \varnothing$.

(b) If $a, b \in \mathbb{Z}$, then $[a, b]$ shall mean the set

$$\begin{aligned}\{a, a+1, a+2, \ldots, b\} &= \{\text{all integers } x \text{ such that } a \leq x \leq b\} \\ &= \{x \in \mathbb{R} \mid a \leq x \leq b\}.\end{aligned}$$

If $a > b$, then this is $\varnothing$.

For example, $[3, 5] = \{3, 4, 5\}$ and $[3, 3] = \{3\}$ and $[5, 3] = \varnothing$.

Now let's define the size of a finite set:

Definition 7.1.2. Let $n \in \mathbb{N}$. A set S is said to have **size** n if S is isomorphic to $[n]$ (that is, if there is a bijection from S to $[n]$).

For example:

- The set {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 between $\mathbb{N}$ and $[n]$ for any $n \in \mathbb{N}$. Thus, $\mathbb{N}$ does not have size n for any $n \in \mathbb{N}$.

Here is another, equivalent definition of size:

> **Definition 7.1.3.** We define the notion of "a set of size n" recursively as follows:
>
> **(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 element $s \in S$ such that $S \setminus \{s\}$ has size $n-1$.

This is a recursive definition, as it reduces the question "what is a set of size n" to the simpler question "what is a set of size $n-1$".

The following fact is not obvious, but can be proved:

> **Theorem 7.1.4.** **(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.

We can now introduce a few notations:

> **Definition 7.1.5.** **(a)** An ***n*-element set** 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)** If S is a finite set, then $|S|$ shall denote the size of S.
>
> **(d)** We also refer to $|S|$ as the **cardinality** of S, or as the **number** of elements of S.

For example,
$$|\{\text{cat, dog, rat}\}| = 3 \qquad \text{and} \qquad |[4,7]| = 4.$$
The # of odd integers between 4 and 8 is
$$|\{\text{odd integers between 4 and 8}\}| = |\{5,7\}| = 2.$$
Recall that sets cannot "contain an element more than once", so $|\{3,5,3\}| = 2$.

7.1.2. Rules for sizes of finite sets

We can now state several common-sense principles that are used all over enumerative combinatorics.

Theorem 7.1.6 (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 7.1.7. For each $n \in \mathbb{N}$, we have $|[n]| = n$.

Theorem 7.1.8. Let S be a set. Then:

(a) We have $|S| = 0$ if and only if $S = \varnothing$ (that is, S is empty).
(b) We have $|S| = 1$ if and only if $S = \{s\}$ for a single element s.
(c) We have $|S| = 2$ if and only if $S = \{s, t\}$ for two distinct elements s and t.

Theorem 7.1.9. Let S be a finite set. Let t be any object such that $t \notin S$. Then,

$$|S \cup \{t\}| = |S| + 1.$$

Theorem 7.1.10 (Sum rule for two sets)**.** Let A and B be two disjoint finite sets. Then, the set $A \cup B$ is again finite, and its size is

$$|A \cup B| = |A| + |B| .$$

Theorem 7.1.11 (Sum rule for k sets)**.** Let $A_1, A_2, \ldots, A_k$ be k disjoint finite sets. Then, the set $A_1 \cup A_2 \cup \cdots \cup A_k$ is again finite, and its size is

$$|A_1 \cup A_2 \cup \cdots \cup A_k| = |A_1| + |A_2| + \cdots + |A_k| .$$

Theorem 7.1.12 (Difference rule)**.** Let T be a subset of a finite set S. Then:
(a) The set T is finite, and its size satisfies $|T| \leq |S|$.
(b) We have $|S \setminus T| = |S| - |T|$.
(c) If $|T| = |S|$, then $T = S$.

Theorem 7.1.13 (Product rule for two sets)**.** Let A and B be any 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 7.1.14 (Product rule for k sets)**.** Let $A_1, A_2, \ldots, A_k$ be any k finite sets. Then, the set

$$\begin{aligned} & A_1 \times A_2 \times \cdots \times A_k \\ & = \{(a_1, a_2, \ldots, a_k) \mid a_i \in A_i \text{ for each } i \in [k]\} \end{aligned}$$

is again finite and has size

$$|A_1 \times A_2 \times \cdots \times A_k| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_k| .$$

The above theorems are basic and can be used to derive further counting rules. For instance:

Corollary 7.1.15. Let A and B be two finite sets (not necessarily disjoint). Then,

$$|A \cup B| = |A| + |B| - |A \cap B| .$$

Corollary 7.1.16. Let A, B and C be three finite sets (not necessarily disjoint). Then,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| .$$

In fact, these two corollaries are the beginning of a pattern: For any k sets $A_1, A_2, \ldots, A_k$, we can write $|A_1 \cup A_2 \cup \cdots \cup A_k|$ as the sum of their sizes $|A_i|$, corrected for all kinds of intersections. This is known as the "principle of inclusion and exclusion" or the "Sylvester sieve formula".

7.2. Redoing some proofs rigorously

Armed with these counting rules, we can now put all our counting proofs on a rigorous footing. Let me only show this on a couple examples (see the notes for more).

First, we recall the following proposition:

Proposition 7.2.1. Let $a, b \in \mathbb{Z}$ be such that $a \leq b + 1$.

Then, there are exactly $b - a + 1$ numbers in the set $[a, b]$. In other words, there are exactly $b - a + 1$ integers between a and b (inclusive).

I said that this can be proved by induction on b, but let us sketch a different proof:

Proof. Consider the map

$$f : \underbrace{[b-a+1]}_{=\{1,2,\ldots,b-a+1\}} \to \underbrace{[a,b]}_{=\{a,a+1,\ldots,b\}}, \\ i \mapsto i+(a-1).$$

This map f just adds $a-1$ to its input.

The map f has an inverse, namely the map

$$g : \underbrace{[a,b]}_{=\{a,a+1,\ldots,b\}} \to \underbrace{[b-a+1]}_{=\{1,2,\ldots,b-a+1\}}, \\ j \mapsto j-(a-1).$$

So f is a bijection. Hence, we have found a bijection from $[b-a+1]$ to $[a,b]$ (namely, f). The bijection principle thus yields

$$|[b-a+1]| = |[a,b]|.$$

Thus,

$$|[a,b]| = |[b-a+1]| = b-a+1.$$

□

Let us return to the theorems that count all subsets of a given set.

Theorem 7.2.2. Let $n \in \mathbb{N}$. Then,

$$(\# \text{ of subsets of } [n]) = 2^n.$$

Rigorous proof. We induct on n.

Base case: The set $[0]$ is empty, and thus has exactly 1 subset. This matches $2^0 = 1$. So the theorem holds for $n = 0$.

Induction step: We proceed from $n-1$ to n. Thus, let n be a positive integer. Assume (as IH) that

$$(\# \text{ of subsets of } [n-1]) = 2^{n-1}.$$

Our goal is to prove that

$$(\# \text{ of subsets of } [n]) \overset{?}{=} 2^n.$$

We define

- a **red set** to be a subset of $[n]$ that contains n;
- a **green set** to be a subset of $[n]$ that does not contain n.

For example, if $n = 3$, then the red sets are

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

whereas the green sets are

$$\{\}, \quad \{1\}, \quad \{2\}, \quad \{1,2\}.$$

Each subset of $[n]$ is either red or green. In other words,

$$\{\text{subsets of } [n]\} = \{\text{red sets}\} \cup \{\text{green sets}\}.$$

But no subset of $[n]$ is simultaneously red and green. Thus, the sets $\{\text{red sets}\}$ and $\{\text{green sets}\}$ are disjoint. Hence, by the sum rule,

$$|\{\text{red sets}\} \cup \{\text{green sets}\}| = |\{\text{red sets}\}| + |\{\text{green sets}\}|.$$

Thus,

$$|\{\text{subsets of } [n]\}| = |\{\text{red sets}\}| + |\{\text{green sets}\}|.$$

In other words,

$$(\text{\# of subsets of } [n]) = (\text{\# of red sets}) + (\text{\# of green sets}).$$

So let us now count the red sets and the green sets separately.

We start with the green sets: These are the subsets of $[n]$ that do not contain n. In other words, they are just the subsets of $[n-1]$. Hence,

$$(\text{\# of green sets}) = (\text{\# of subsets of } [n-1]) = 2^{n-1}.$$

Let us now count the red sets. These are just the green sets, with an n inserted into them. More precisely: Each green set can be turned into a red set by inserting n into it. Conversely, each red set can be turned green by removing n from it. Thus we obtain two maps

$$\begin{aligned} \operatorname{ins}_n : \{\text{green sets}\} &\to \{\text{red sets}\}, \\ G &\mapsto G \cup \{n\} \end{aligned}$$

and

$$\begin{aligned} \operatorname{rem}_n : \{\text{red sets}\} &\to \{\text{green sets}\}, \\ R &\mapsto R \setminus \{n\}. \end{aligned}$$

It is clear that these maps ins_n and rem_n are inverses of each other. Hence, the map rem_n has an inverse, and thus is a bijection. Therefore, by the bijection principle,

$$|\{\text{red sets}\}| = |\{\text{green sets}\}|.$$

In other words,

$$(\text{\# of red sets}) = (\text{\# of green sets}) = 2^{n-1}.$$

Altogether,

$$\begin{aligned}(\text{\# of subsets of } [n]) &= \underbrace{(\text{\# of red sets})}_{=2^{n-1}} + \underbrace{(\text{\# of green sets})}_{=2^{n-1}} \\ &= 2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n.\end{aligned}$$

This completes the induction step. Thus, the theorem is proved. □

More generally:

> **Theorem 7.2.3.** Let $n \in \mathbb{N}$. Let S be an n-element set. Then,
>
> $$(\text{\# of subsets of } S) = 2^n.$$

Rigorous proof. Informally, we derived this from the preceding theorem by renaming the elements of S as $1, 2, \ldots, n$ and arguing that the subsets of S then become the subsets of $[n]$.

To make this rigorous, we set up a bijection between S and $[n]$, and then we apply this bijection elementwise to the subsets.

In detail: The set S has size n. In other words, S is isomorphic to $[n]$. Thus, there exists a bijection $\alpha : S \to [n]$. Consider this α. As a bijection, α has an inverse α^{-1}.

Now, we define a map

$$\begin{aligned}\alpha_* : \{\text{subsets of } S\} &\to \{\text{subsets of } [n]\}, \\ T &\mapsto \{\alpha(t) \mid t \in T\}.\end{aligned}$$

This map α_* is a bijection, because it has an inverse $\left(\alpha^{-1}\right)_*$ (constructed in the same way as α_*, but using α^{-1} instead of α).

So the bijection principle yields

$$|\{\text{subsets of } S\}| = |\{\text{subsets of } [n]\}|.$$

In other words,

$$(\text{\# of subsets of } S) = (\text{\# of subsets of } [n]) = 2^n$$

(by the previous theorem). □

7.3. Lacunar subsets

Another type of objects we can count are the so-called **lacunar subsets**:

Definition 7.3.1. A set S of integers is said to be **lacunar** if it contains no two consecutive integers (i.e., if there exists no integer i such that both i and $i+1$ belong to S).

For example, $\{2,4,7\}$ is lacunar, whereas $\{1,2\}$ and $\{1,2,5\}$ are not. Any 1-element set of integers is lacunar, and so is the empty set.

Now we can ask ourselves three natural questions: 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 $[n]$ have for a given k ?

3. what is the largest size of a lacunar subset of $[n]$?

Let us answer all these three questions, starting with the easiest one, which is Question 3:

Proposition 7.3.2. 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. See the notes (but pretty easy). □

Let us come to Question 1: We can easily generate a lot of data:

n	0	1	2	3	4	5	6	7	8
# of lacunar subsets of $[n]$	1	2	3	5	8	13	21	34	55

For example, for $n = 4$, the lacunar subsets of $[4]$ are

$$\varnothing, \ \{1\}, \ \{2\}, \ \{3\}, \ \{4\}, \ \{1,3\}, \ \{1,4\}, \ \{2,4\}.$$

So we suspect:

Theorem 7.3.3. For any integer $n \geq -1$, we have

$$(\text{\# of lacunar subsets of } [n]) = f_{n+2},$$

where f_i denotes the i-th Fibonacci number. Here, we agree that $[-1] := \varnothing$, and more generally, $[k] := \varnothing$ for all $k \leq 0$.

Proof. For any integer $n \geq -1$, let us set

$$\ell_n := (\text{\# of lacunar subsets of } [n]).$$

So our goal is to prove that $\ell_n = f_{n+2}$ for every integer $n \geq -1$.

We observe that $\ell_{-1} = 1 = f_1$ and $\ell_0 = 1 = f_2$. So the theorem holds for $n = -1$ and for $n = 0$.

We will now show that the sequence $(\ell_{-1}, \ell_0, \ell_1, \ldots)$ satisfies the same recursion as the Fibonacci sequence:

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.

Then, the definition of ℓ_n shows that

$$\begin{aligned} \ell_n &= (\text{\# of lacunar subsets of } [n]) \\ &= (\text{\# of red lacunar subsets of } [n]) + (\text{\# of green lacunar subsets of } [n]) . \end{aligned}$$

So we need to count the lacunar subsets of each color.

The green ones are easy: The green lacunar subsets of $[n]$ are the lacunar subsets of $[n-1]$. Thus,

$$\begin{aligned} &(\text{\# of green lacunar subsets of } [n]) \\ &= (\text{\# of lacunar subsets of } [n-1]) = \ell_{n-1}. \end{aligned}$$

What about the red ones? If we remove n from a red lacunar subset of $[n]$, then we obtain a lacunar subset of $[n-2]$ (since the original red lacunar subset contained n and thus could not have contained $n-1$ due to its lacunarity). Conversely, if we insert n into a lacunar subset of $[n-2]$, we get a red lacunar subset of $[n]$ (since the lack of $n-1$ in our subset creates a "buffer zone" so that the newly inserted n does not have a neighbor). So we obtain two maps

$$\begin{aligned} \operatorname{rem}_n : \{\text{red lacunar subsets of } [n]\} &\to \{\text{lacunar subsets of } [n-2]\} , \\ R &\mapsto R \setminus \{n\} \end{aligned}$$

and

$$\begin{aligned} \operatorname{ins}_n : \{\text{lacunar subsets of } [n-2]\} &\to \{\text{red lacunar subsets of } [n]\} , \\ L &\mapsto L \cup \{n\} , \end{aligned}$$

which are obviously inverses of each other. Thus, they are bijections, and 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, we now have

$$\begin{aligned} \ell_n &= \underbrace{(\text{\# of red lacunar subsets of } [n])}_{=\ell_{n-2}} + \underbrace{(\text{\# of green lacunar subsets of } [n])}_{=\ell_{n-1}} \\ &= \ell_{n-2} + \ell_{n-1} = \ell_{n-1} + \ell_{n-2}. \end{aligned}$$

This proves Claim 1. □

Now recall that our goal is to show that the sequences $(\ell_{-1}, \ell_0, \ell_1, \ldots)$ and $(f_1, f_2, f_3, \ldots)$ are identical. But at this point, this is very easy: These two sequences

- have the same two starting entries ($\ell_{-1} = f_1$ and $\ell_0 = f_2$),
- and satisfy the same recursive equation: namely, each entry of either sequence is the sum of the preceding two (by Claim 1).

So the sequences must be equal. □

The remaining one of the three questions about lacunar subsets was: How many lacunar subsets does $[n]$ have of a given size k ?

Theorem 7.3.4. Let $n \in \mathbb{Z}$ and $k \in \mathbb{N}$ be such that $k \leq n+1$. Then,

$$(\text{\# of } k\text{-element lacunar subsets of } [n]) = \binom{n+1-k}{k}.$$

Proof. One way to prove this is by induction on n, using red and green colors as before.

A nicer proof proceeds using the bijection principle. We construct a bijection

$$\begin{aligned}&\text{from } \{k\text{-element lacunar subsets of } [n]\} \\ &\text{to } \{k\text{-element subsets of } [n+1-k]\}.\end{aligned}$$

Namely, this bijection sends each k-element lacunar subset $S = \{s_1 < s_2 < \cdots < s_k\}$ of $[n]$ (this notation means that the elements of S are called $s_1, s_2, \ldots, s_k$ in increasing order) to the k-element subset

$$\{s_1 - 0,\ s_2 - 1,\ s_3 - 2,\ \ldots,\ s_k - (k-1)\} \text{ of } [n+1-k].$$

In other words, the elements of S get "squeezed together" in that the distance between any two consecutive elements gets shrunk by 1. This operation preserves the relative order of these elements, in the sense that

$$s_1 - 0 < s_2 - 1 < s_3 - 2 < \cdots < s_k - (k-1)$$

(since S is lacunar).

This map is bijective, because it has an inverse: namely, the map

$$\begin{aligned}&\text{from } \{k\text{-element subsets of } [n+1-k]\} \\ &\text{to } \{k\text{-element lacunar subsets of } [n]\}\end{aligned}$$

that sends each k-element subset $\{t_1 < t_2 < \cdots < t_k\}$ of $[n+1-k]$ to

$$\{t_1 + 0,\ t_2 + 1,\ t_3 + 2,\ \ldots,\ t_k + (k-1)\}.$$

Thus, the bijection principle yields

$$\begin{aligned}&(\text{\# of } k\text{-element lacunar subsets of } [n])\\ &= (\text{\# of } k\text{-element subsets of } [n+1-k])\\ &= \binom{n+1-k}{k} \qquad \left(\begin{array}{c}\text{by the combinatorial}\\ \text{interpretation of BCs}\end{array}\right).\end{aligned}$$

□

So we have now answered all three questions about lacunar subsets: how big they can get, how many there are, and how many have a given size. As for the second question, we actually obtain two different answers:

On the one hand, we have shown that

$$(\text{\# of lacunar subsets of } [n]) = f_{n+2}.$$

On the other hand, by the sum rule,

$$\begin{aligned}&(\text{\# of lacunar subsets of } [n])\\ &= \sum_{k=0}^{n+1} \underbrace{(\text{\# of } k\text{-element lacunar subsets of } [n])}_{=\binom{n+1-k}{k}}\\ &= \sum_{k=0}^{n+1} \binom{n+1-k}{k}.\end{aligned}$$

Comparing these equalities, we obtain

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

If we substitute $n-1$ for n in this equality, it becomes:

Corollary 7.3.5. Let $n \in \mathbb{N}$. Then, the Fibonacci number f_{n+1} is

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

7.4. Compositions and weak compositions

7.4.1. Compositions

How many ways are there to write the number 5 as a sum of 3 positive integers, if the order matters?

$$\begin{aligned} 5 &= 2+2+1 = 2+1+2 = 1+2+2 \\ &= 3+1+1 = 1+3+1 = 1+1+3. \end{aligned}$$

So there are 6 such ways.

What about the general case?

Definition 7.4.1. **(a)** If $n \in \mathbb{N}$, then a **composition** of n shall mean a tuple (i.e., finite list) of positive integers whose sum is n.

(b) If $n, k \in \mathbb{N}$, then a **composition of n into k parts** shall mean a k-tuple of positive integers whose sum is n.

(This is old terminology and has nothing to do with compositions of maps.)

For example, the compositions of 5 into 3 parts are

$$(2,2,1), \quad (2,1,2), \quad (1,2,2), \quad (3,1,1), \quad (1,3,1), \quad (1,1,3).$$

The compositions of 3 are

$$(3), \quad (2,1), \quad (1,2), \quad (1,1,1).$$

The only composition of 0 is the 0-tuple $()$, which is a composition into 0 parts.

Let us now count compositions of n into k parts.

Theorem 7.4.2. Let $n, k \in \mathbb{N}$. Then,

$$(\text{\# of compositions of } n \text{ into } k \text{ parts}) = \binom{n-1}{n-k}.$$

If $n > 0$, then

$$(\text{\# of compositions of } n \text{ into } k \text{ parts}) = \binom{n-1}{k-1}.$$

Proof. The case $n = 0$ is very easy, so we just omit it. Thus, WLOG assume that $n > 0$. Thus, $n - 1 \in \mathbb{N}$.

We are looking for a bijection

$$\begin{aligned} &\text{from } \{\text{compositions of } n \text{ into } k \text{ parts}\} \\ &\text{to } \{(k-1)\text{-element subsets of } [n-1]\}. \end{aligned}$$

Such a bijection can be constructed as follows: It sends every composition $a = (a_1, a_2, \ldots, a_k)$ of n to the subset

$$\{a_1, \ a_1 + a_2, \ a_1 + a_2 + a_3, \ \ldots, \ a_1 + a_2 + \cdots + a_{k-1}\}.$$

To prove that this is a bijection, we have to construct its inverse. This inverse sends a $(k-1)$-element subset $S = \{s_1 < s_2 < \cdots < s_{k-1}\}$ to the composition

$$(s_1, \ s_2 - s_1, \ s_3 - s_2, \ s_4 - s_3, \ \ldots, \ s_{k-1} - s_{k-2}, \ n - s_k).$$

Thus the bijection principle yields

$$\begin{aligned}
&(\text{\# of compositions of } n \text{ into } k \text{ parts}) \\
&= (\text{\# of } (k-1)\text{-element subsets of } [n-1]) \\
&= \binom{n-1}{k-1} \qquad \left(\begin{array}{c}\text{by the combinatorial}\\ \text{interpretation of BCs}\end{array}\right) \\
&= \binom{n-1}{(n-1)-(k-1)} \qquad \left(\begin{array}{c}\text{by the symmetry}\\ \text{of BCs}\end{array}\right) \\
&= \binom{n-1}{n-k}.
\end{aligned}$$

□

Theorem 7.4.3. Let n be a positive integer. Then, the # of all compositions of n is 2^{n-1}.

Proof. Same idea as above, but now we no longer restrict to k parts / $k-1$ elements. □

7.4.2. Weak compositions

If we extend the notion of a composition to allow 0's as entries, then we end up with **weak compositions**:

Definition 7.4.4. (a) If $n \in \mathbb{N}$, then a **weak composition** of n shall mean a tuple (i.e., finite list) of nonnegative integers whose sum is n.

(b) If $n, k \in \mathbb{N}$, then a **weak composition of** n **into** k **parts** shall mean a k-tuple of nonnegative integers whose sum is n.

For instance, the weak compositions of 2 into 3 parts are

$$(1,1,0), \quad (1,0,1), \quad (0,1,1), \quad (2,0,0), \quad (0,2,0), \quad (0,0,2).$$

It makes little sense to ask for the # of all weak compositions of n, since there are ∞ of them (for example, 0 has weak compositions $()$, (0), $(0,0)$, $(0,0,0)$, and so on). But we can ask for the # of all weak compositions of n into k parts:

Theorem 7.4.5. Let $n, k \in \mathbb{N}$. Then,

$$(\text{\# of weak compositions of } n \text{ into } k \text{ parts}) = \binom{n+k-1}{n}.$$

Proof. Consider the bijection

$$\begin{aligned}&\text{from } \{\text{weak compositions of } n \text{ into } k \text{ parts}\}\\ &\text{to } \{\text{compositions of } n+k \text{ into } k \text{ parts}\}\end{aligned}$$

which sends

$$(a_1, a_2, \ldots, a_k) \mapsto (a_1 + 1,\ a_2 + 1,\ \ldots,\ a_k + 1).$$

Its inverse map sends

$$(b_1, b_2, \ldots, b_k) \mapsto (b_1 - 1,\ b_2 - 1,\ \ldots,\ b_k - 1).$$

So the bijection principle yields

$$\begin{aligned}&(\text{\# of weak compositions of } n \text{ into } k \text{ parts})\\ &= (\text{\# of composition of } n+k \text{ into } k \text{ parts})\\ &= \binom{n+k-1}{n+k-k} \qquad \text{(by a previously proved theorem)}\\ &= \binom{n+k-1}{n}.\end{aligned}$$

□

7.5. Selections

Here is a classical question we posed a few chapters ago and haven't fully addressed yet: How many ways are there to select k elements from a given n-element set S ?

The words "k elements" here can be interpreted in 4 different ways, leading to 4 different problems. Here are the choices you can make:

1. Do we want k arbitrary elements or k distinct elements?

2. Does the order of these k elements matter or not? (E.g., do we count "1, 2" and "2, 1" as two different selections?)

Let us explore these 4 options now.

7.5.1. Unordered selections without repetition (= without replacement)

To select k distinct elements from S without regard for their order is the same as selecting a k-element subset of S. We know how to count them:

Theorem 7.5.1. Let $n \in \mathbb{N}$, and let k be any number. Let S be an n-element set. Then,

$$(\text{\# of } k\text{-element subsets of } S) = \binom{n}{k}.$$

7.5.2. Ordered selections without repetition

Now, let us consider the question of selecting k distinct elements from a set S with regard to their order. This kind of selections is best described as k-tuples of a specific kind: what I call "injective k-tuples".

Definition 7.5.2. Let $k \in \mathbb{N}$. 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 $i_a \neq i_b$ whenever $a \neq b$).

For example, $(3, 1, 5)$ is injective, but $(3, 1, 3)$ is not.

Definition 7.5.3. Let S be any set, and let $k \in \mathbb{N}$. Then, S^k shall mean the Cartesian product

$$\begin{aligned}\underbrace{S \times S \times \cdots \times S}_{k \text{ times}} &= \{(a_1, a_2, \ldots, a_k) \mid a_1, a_2, \ldots, a_k \in S\} \\ &= \{k\text{-tuples whose all entries belong to } S\}.\end{aligned}$$

Now, our counting problem becomes the question of counting the injective k-tuples in S^k. Here is the answer:

Theorem 7.5.4. Let $n, k \in \mathbb{N}$. Let S be an n-element set. Then,

$$\begin{aligned}\left(\text{\# of injective } k\text{-tuples in } S^k\right) &= n(n-1)(n-2)\cdots(n-k+1) \\ &= \binom{n}{k} \cdot k! \\ &= \frac{n!}{(n-k)!} \qquad \text{if } k \leq n.\end{aligned}$$

Informal proof. (See the notes for a rigorous proof.)

Example: Let $n = 5$ and $k = 3$ and $S = \{a, b, c, d, e\}$. We must count the injective k-tuples in S^k, that is, the injective 3-tuples in S^3. These are the triples (x, y, z) of distinct elements of S. Here is a way to choose such a triple:

1. First, we choose its first entry x. There are 5 options for this, since S has 5 elements.
2. Next, we choose its second entry y. There are 4 options for this, since y can be any of the 5 elements of S except for x (since the injectivity of (x, y, z) requires $y \neq x$).
3. Finally, we choose its third entry z. There are 3 options for this, since z can be any of the 5 elements of S except for x and y (and x and y are distinct).

Altogether, we have 5 options at the first step, 4 at the second, and 3 at the third. This gives rise to $5 \cdot 4 \cdot 3$ possible outcomes, and each outcome gives a different 3-tuple, and each 3-tuple really is obtained this way. So the total # of injective 3-tuples is $5 \cdot 4 \cdot 3 = 60$.

The general case is similar. What we are tacitly using is a counting rule called the **dependent product rule**, which (informally) states that if we perform a multi-step construction, and we have

- exactly n_1 options in step 1,
- exactly n_2 options in step 2,
- $\ldots$,
- exactly n_k options in step k,

then the entire construction can be performed in $n_1 n_2 \cdots n_k$ many different ways. Usually, proofs that use this rule can be rewritten as induction proofs (inducting on k). In particular, in the notes, I do this with the proof above. □

7.5.3. Intermezzo: Listing n elements

If we apply the above theorem to $k = n$, then we conclude that the # of ways to choose n distinct elements from an n-element set S, where the order matters, is

$$n(n-1)(n-2)\cdots(n-n+1) = n(n-1)(n-2)\cdots 1 = n!.$$

Of course, when you choose n distinct elements from an n-element set S, you necessarily must choose all the elements of S. So these ways are just ways of listing the n elements of S in some order. So we have obtained:

> **Corollary 7.5.5.** 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 of elements of S that contain each element of S exactly once) is $n!$.

For example, the ways to list the 3 elements of $[3]$ are

$$(1,2,3), \quad (1,3,2), \quad (2,1,3), \quad (2,3,1), \quad (3,1,2), \quad (3,2,1).$$

7.5.4. Ordered selections with repetition

The ways to select k elements from an n-element set S, if the order matters, are simply the k-tuples of elements of S. Their # is

$$\underbrace{nn\cdots n}_{k \text{ times}} = n^k.$$

So we have shown:

Theorem 7.5.6. Let $n, k \in \mathbb{N}$. Let S be an n-element set. Then,

$$\left(\text{\# of all } k\text{-tuples in } S^k\right) = n^k.$$

7.5.5. Unordered selections with repetition

Now only one question remains: 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 ways to rigorously define what this means:

1. We can define the notion of a **multiset**, which is "like a finite set but allowing for repeated elements". This is usually done in combinatorics courses (Math 222).
2. Alternatively, we can define the notion of an **unordered k-tuple**, which is a "k-tuple up to reordering its entries". Rigorously, it is an equivalence class of k-tuples with respect to the relation of "being a permutation of". This is the algebraic approach (see classes on abstract algebra).
3. The most pedestrian way: We restrict ourselves to the case $S = [n]$, and we count only the **weakly increasing** k-tuples – i.e., the k-tuples $(i_1, i_2, \ldots, i_k)$ that satisfy $i_1 \leq i_2 \leq \cdots \leq i_k$.

These three definitions yield different but equivalent objects ("equivalent" meaning here that there are bijections between from each kind of object to each other). So the #s of these objects are the same. Here is a formula for these #s:

Theorem 7.5.7. Let $n, k \in \mathbb{N}$. Let S be an n-element set. Then,

$$\begin{aligned}&(\text{\# of all ways to select } k \text{ elements from } S \text{ (if order does not matter)})\\ &= \binom{k+n-1}{k}.\end{aligned}$$

See the notes for a proof.

See the notes also for a few other counting problems.