Math 221 Section 5 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

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

The major topics we will cover in this course are

- **mathematical induction** and **recursion**;
- **elementary number theory** (divisibility, prime numbers, coprimality);
- basic **enumerative combinatorics** (counting and binomial coefficients);
- basic **combinatorial game theory**.

We will not go very deep, nor will we be fully rigorous. See the notes for references that elaborate on these topics.

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, and these disks have different sizes, stacked from largest to smallest as you go up. 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 disks currently on the latter peg. In other words, you cannot stack a bigger disk atop a smaller one.

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

This game can be played online in many places (e.g. https://codepen.io/eliortabeka/pen/yOrrx).

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

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

This strategy wins the game in 7 moves for $n = 3$.

What about other values of n ? The questions are:

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 disks – all 0 of them – are on peg 3 already).
- For $n = 1$, we win in 1 move.
- For $n = 2$, we win in 3 moves.

- For $n = 3$, our above strategy wins in 7 moves, but maybe we can do better?

Solving the game by brute force gets more and more tiresome as n grows larger. So let us try to spot a pattern in our strategies for small n's, and see if it holds on for higher n's.

The $n = 3$ strategy seems to follow a pattern: Its first 3 steps are freeing the biggest disk; the next step moves the biggest disk from peg 1 to peg 3; the last 3 steps are again placing the other disks on top of it. So we can rewrite our $n = 3$ strategy as follows:

1.–3. Move the two smaller disks from peg 1 onto peg 2. (This is essentially a Tower of Hanoi puzzle 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.)

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

5.–7. Move the two smaller disks from peg 2 onto peg 3. (This is again a Tower of Hanoi puzzle played only with the two smaller disks.)

Now the logic behind the above strategy has become clear.

Let us try to adapt this same logic to the $n = 4$ case:

1.–7. Move the three smaller disks from peg 1 onto peg 2. (This is essentially a Tower of Hanoi puzzle played only with the three smaller disks.)

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

9.–15. Move the three smaller disks from peg 2 onto peg 3.

As you see, we don't just have a strategy for $n = 3$ and a strategy for $n = 4$. We have a "meta-strategy" that lets us win the game for n disks if we know how to win it for $n - 1$ disks. We shall still refer to it as "strategy".

Let us summarize what we gain from this strategy.

Definition 1.1.2. For any integer $n \geq 0$, we let m_n denote the # of moves needed to win with n disks. If the game cannot 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.

Let us make a little table of small values of m_n obtained using our strategy:

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

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 an extra move, and then win it for $n-1$ again. So we get

$$m_n = m_{n-1} + 1 + m_{n-1} = 2m_{n-1} + 1 \qquad \text{for all } n \geq 1.$$

Right?

Not so fast. We have defined m_n to be the smallest # of moves needed to solve the game. But what we have computed is the smallest # of moves needed to solve the game **using our strategy**. What if our strategy is not the quickest way? Then the true m_n would be smaller than the one we have found.

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 $m_n \leq 2m_{n-1} + 1$.

To practice some mathematical writing, let us spell the proof out in detail:

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

A. We use 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 because this disk is free (i.e., has no disks on top of it) and because peg 3 is empty (since all other disks are on peg 2).)

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

This strategy wins the game (for n disks) in $m_{n-1} + 1 + m_{n-1} = 2m_{n-1} + 1$ many moves. So the game for n disks can be won in $2m_{n-1} + 1$ moves. In other words, $m_n \leq 2m_{n-1} + 1$. Qed. □

Now, let us see if the inequality $m_n \leq 2m_{n-1}+1$ is an equality or just an inequality – i.e., whether our above strategy is optimal or there is a faster one. I claim that it 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, we assume that m_{n-1} is an integer.

We need to show that $m_n = 2m_{n-1}+1$. It suffices to show that $m_n \geq 2m_{n-1}+1$, since our previous proposition says that $m_n \leq 2m_{n-1}+1$. 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 T, the largest disk has to move. Let us refer to these moves (i.e., the moves that move the largest disk) as **special moves**. There may be one of them or more, but there has to be **at least** one.

Before the first special move can happen, the smallest $n-1$ disks have to all be moved on the same peg which is either peg 2 or peg 3 (since otherwise, the largest disk could either not be lifted or not be placed). Thus, before the first special move can happen, we must have won the Tower of Hanoi game for $n-1$ disks. So we need to make at least m_{n-1} moves before our first special move.

Now, consider what happens **after the last special move**. This last special move necessarily moves the largest disk to peg 3. After that, we still need to move all the other disks onto peg 3. We note that at the time of the last special move, all these other disks must be on the same peg, since otherwise the largest disk could not be moved. So we still need to win the Tower of Hanoi game for $n-1$ disks. For this we need at least m_{n-1} moves.

Altogether, we see that 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.

So, altogether, it has to contain at least $m_{n-1}+1+m_{n-1} = 2m_{n-1}+1$ moves. This proves $m_n \geq 2m_{n-1}+1$. Qed. □

So this proposition confirms the table we have carelessly made before:

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

A look at this table suggests that maybe there is an **explicit formula** for m_n (that is, a formula that gives m_n directly, without having to compute $m_0, m_1, \ldots, m_{n-1}$ first). Namely, it suggests that

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

For example, you can spot it by computing ratios between consecutive entries:

$$\begin{aligned} \frac{m_8}{m_7} &= \frac{255}{127} \approx 2.0079; \\ \frac{m_9}{m_8} &= \frac{511}{255} \approx 2.0039; \\ &\ldots, \end{aligned}$$

which suggest that $m_n \approx 2^n$, and then you can easily spot the pattern in the difference $m_n - 2^n$.

I claim that the above formula $m_n = 2^n - 1$ is actually true. How could this be proved?

Our above proposition shows that if $m_{n-1} \neq \infty$, then $m_n = 2m_{n-1} + 1$. Thus, if the formula $m_{n-1} = 2^{n-1} - 1$, then

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

In other words, if our claimed formula $m_n = 2^n - 1$ is true for $n - 1$ instead of n, then it is true for n as well. In particular:

- If $m_0 = 2^0 - 1$, then $m_1 = 2^1 - 1$. So we get $m_1 = 2^1 - 1$ (since $m_0 = 2^0 - 1$).
- If $m_1 = 2^1 - 1$, then $m_2 = 2^2 - 1$. So we get $m_2 = 2^2 - 1$ (since $m_1 = 2^1 - 1$).
- If $m_2 = 2^2 - 1$, then $m_3 = 2^3 - 1$. So we get $m_3 = 2^3 - 1$ (since $m_2 = 2^2 - 1$).
- .....
- If $m_{1006} = 2^{1006} - 1$, then $m_{1007} = 2^{1007} - 1$. So we get $m_{1007} = 2^{1007} - 1$.
- .....

Using this kind of reasoning, for any given $n \geq 0$, you can prove that $m_n = 2^n - 1$ by n such steps (starting with $m_0 = 2^0 - 1$, then moving on to show $m_1 = 2^1 - 1$, then to show $m_2 = 2^2 - 1$, and so on, until you get to m_n).

Common sense dictates that this should constitute a proof of $m_n = 2^n - 1$ for each $n \geq 0$. To make this formal, we have to state a principle (an axiom) that underlies this kind of reasoning. This is the **Principle of Mathematical Induction**:

Theorem 1.1.5 (Principle of Mathematical Induction)**.** Let b be an integer.

Let $P(n)$ be a mathematical statement defined for each integer $n \geq b$.

(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". 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 $P(b)$ holds (i.e., $P(n)$ holds for $n = b$).
2. For each integer $n \geq b$, the implication $P(n) \implies P(n+1)$ holds (i.e., if $P(n)$ holds, then $P(n+1)$ holds as well).

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

Let me recall the meaning of the "$\implies$" symbol: An implication $A \implies B$ holds whenever B is true or A is false, but not in the remaining case (i.e., when A is true but B is false). Thus, for example, "$0 = 1 \implies 16$ is prime" is true. The truth table of implication is as follows:

A	B	$A \implies B$
true	true	true
true	false	false
false	true	true
false	false	true

.

Next time, we will apply the Principle of Mathematical Induction to prove that

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

1.2. The Principle of Mathematical Induction

Repeating:

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

Let $P(n)$ be a mathematical statement 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 so does $P(n+1)$).

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

Before we say more about the role and meaning of this principle, let me show how to use it to prove our $m_n \stackrel{?}{=} 2^n - 1$ conjecture from last time:

Theorem 1.2.2 (explicit answer to Tower of Hanoi)**.** For each integer n, we let m_n be the # of moves needed to win the Tower of Hanoi game (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 $P(n)$. Thus, 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.

To prove these two claims will be our two goals; we call them Goal 1 and Goal 2. Let us see if we can achieve them.

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

Let us now work towards Goal 2. Let $n \geq 0$ be an integer. We must prove the implication $P(n) \Longrightarrow P(n+1)$. To prove this, 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, so that the Hanoi game for n disks is winnable.

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

The last proposition we showed says that $m_n = 2m_{n-1} + 1$ if $n \geq 1$.

But we can also apply this proposition to $n+1$ instead of n (since the n in the proposition was an arbitrary positive integer; it does not have to coincide with our current n). Thus, we get

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

Thus,

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

which is exactly the statement $P(n+1)$ we wanted to prove. So goal 2 is achieved.

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

What has really happened here? How did this proof work?

Let us take a look at the structure of this 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

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

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

We have then proved that $P(n) \Longrightarrow P(n+1)$ for each n. In other words, we have proved that $P(0) \Longrightarrow P(1)$ 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 obtain $P(1)$.

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

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

Etc. Continuing this way, you can obtain $P(n)$ for each $n \geq 0$, although you need more and more steps the larger n becomes. Common sense tells you that this should qualify as a proof of $P(n)$ for all n. The Principle of Mathematical Induction simply formalizes this common sense. So, if you want to use this reasoning in a mathematical proof, you have to use the Principle of Mathematical Induction.

Some metaphors:

- You can think of a proof by the Principle of Mathematical Induction as a daisy chain of lamps, which stand for $P(0),\ P(1),\ P(2),\ \ldots$. Goal 1 turns the first lamp on. Goal 2 ensures that each lamp, when turned on, also turns the next lamp on.
- You can also think of it as a sequence of dominos arranged in a row, at sufficiently close distances so that tipping over one will kick down the next. After you tip over the first domino, all the others will eventually fall down.

I called the Principle of Mathematical Induction a theorem, but really it is an axiom of mathematics. Some authors do prove it, but they do so relying on some other axioms that formalize the same intuition.

1.3. Some more proofs by induction

A proof that uses the Principle of Mathematical Induction (such as the proof we gave above) is called a **proof by induction** or an **inductive proof**.

Let us see some more proofs by induction.

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

First proof of the Little Gauss formula. We define

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

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

Let us denote the statement "$s_n = \dfrac{n(n+1)}{2}$" 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 must show that $s_0 = \dfrac{0(0+1)}{2}$, but this is clear since both sides are 0.

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

By assumption, $P(n)$ holds. In other words,

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

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

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

To do so, we observe that

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

In other words, $P(n+1)$ holds. This proves 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 $n \geq 0$, which is exactly what the theorem claims. □

There is a non-inductive proof (supposedly how Gauss figured it out):

Second proof of the Little Gauss formula. We have

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

so that $1+2+\cdots+n = \dfrac{n\cdot(n+1)}{2}$, 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. The following proof is a verbatim copy of the first proof of Little Gauss, just with some necessary changes made.

We define

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

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

Let us denote the 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 $P(n) \implies P(n+1)$ holds.

For Goal 1, we must show that $s_0 = \dfrac{0(0+1)(2\cdot 0+1)}{6}$, but this is clear since both sides are 0.

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

By assumption, $P(n)$ holds. In other words,

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

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

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

To do so, we observe that

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

In other words, $P(n+1)$ holds. This proves the implication $P(n) \implies P(n+1)$.

We have now achieved both goals. So the Principle of Mathematical Induction yields that $P(n)$ holds for each $n \geq 0$, which is exactly what the theorem claims. □

As we said, this proof was an almost-verbatim copy of the first proof of Little Gauss. In contrast, the nice second proof of Little Gauss cannot be extended to $1^2 + 2^2 + \cdots + n^2$.

Exercise 1.3.1. Prove that

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

for each integer $n \geq 0$.

1.4. Notations for an induction proof

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

- The n is called the **induction variable**; you say that you **induct on** n. This variable doesn't have to be called n. Your statement might just as well be proving "for every integer $a \geq 0$, we have $1 + 2 + \cdots + a = \dfrac{a(a+1)}{2}$", and then you can prove it by inducting on a.
- The proof of $P(b)$ (that is, Goal 1 in our above proofs) is called the **induction base** or the **base case**. In our above examples, this was always the proof of $P(0)$, but in general b can be another integer. For example, if you are proving the statement "every integer $n \geq 4$ satisfies $2^n \geq n^2$", then b will have to be 4, so your induction base consists in proving that $2^4 \geq 4^2$.
- The proof of "$P(n) \Longrightarrow P(n+1)$ for each $n \geq b$" (that is, Goal 2 in our above proofs) is called the **induction step**. For example, in the last proof, this was the part where we assumed that

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

  and proved that

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

  In the induction step, the assumption that $P(n)$ holds is called the **induction hypothesis** or the **induction assumption**, and the claim that $P(n+1)$ holds 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 Hanoi theorem using this language:

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

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

Rewritten proof. We induct on n.

Base case: The theorem holds for $n = 0$, since both m_0 and $2^0 - 1$ are 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 will now show that the theorem holds for $n+1$ as well (this is what we previously 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 $m_{n+1} \stackrel{?}{=} 2^{n+1} - 1$. This is our induction goal.

To prove this, we apply the previous proposition (the one that says $m_n = 2m_{n-1} + 1$) to $n+1$ instead of n (we can do this, since $m_n = 2^n - 1$ is not ∞), and obtain

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

Thus, the induction goal is reached, so the induction is complete. Hence, 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**. This sequence is defined **recursively** – i.e., a given entry is not defined directly, but rather is defined in terms of the previous entries. Here is the definition:

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

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

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

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

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

.

As we see, a recursive definition is a perfectly valid way to define (e.g.) a sequence of numbers.

1.5.2. The sum of the first n positive Fibonacci numbers

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

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

For example, for $n = 8$, this is saying that $1 + 1 + 2 + 3 + 5 + 8 + 21 = 55 - 1$.

Proof. We induct on n.

Base case: For $n = 0$, the theorem claims that $f_1 + f_2 + \cdots + f_0 = f_{0+2} - 1$. The left hand side is an empty sum, thus equals 0. The right hand side is $f_2 - 1 = 1 - 1 = 0$. So the theorem holds for $n = 0$.

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

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

We must prove that $f_1 + f_2 + \cdots + f_{n+1} \stackrel{?}{=} f_{n+1+2} - 1$.

We have

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

This completes the induction step. Thus, the theorem is proved. □

1.6. Some more examples of induction

Let us see some more examples of proofs by induction.

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

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

Proof. We induct on n.

Base case: For $n = 0$, the theorem says that an empty sum equals $2^0 - 1 = 0$, which is true.

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 also holds for $n+1$, i.e., that we have

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

But

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

which is precisely what we want. Thus, the theorem holds for $n+1$, so the induction step is complete. The theorem is proved. □

The theorem we just proved 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 $x^i y^j$ where i and j are nonnegative integers satisfying $i + j = n - 1$.

For example:

- For $n = 2$, this theorem says that

$$(x-y)(x+y) = x^2 - y^2.$$

- For $n = 3$, this theorem says that

$$(x-y)\left(x^2+xy+y^2\right) = x^3 - y^3.$$

- For $n = 4$, this theorem says that

$$(x-y)\left(x^3+x^2y+xy^2+y^3\right) = x^4 - y^4.$$

- For $x = 2$ and $y = 1$, this theorem says that

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

  Since any power of 1 is 1, and since $2-1=1$, this simplifies to

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

  In other words,

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

  This is the previous theorem.

Let us now prove the generalized 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 saying that $(x-y)\,(\text{an empty sum}) = x^0 - y^0$, which is true because both sides are 0.

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

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

We must prove that the theorem is true for $n+1$ as well. In other words, 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 in the second pair of parentheses on the LHS. We thus obtain

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

which is precisely the induction goal. 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 $y=1$. We get

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

Simplifying this, we find

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

Thus,

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

But the LHS is $q^0+q^1+q^2+\cdots+q^{n-1}$, written in reverse. □

1.7. How not to 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: The theorem holds for $n = 1$, since a single horse has only one color.

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

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

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

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

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

Now, consider the first horse H_1 and the last horse H_{n+1}. They both have the same color as the "middle horses" $H_2, H_3, \ldots, H_n$ (by the preceding two paragraphs). So all $n+1$ horses have the same color. "Qed."

What went wrong?

There is an easy way to debug a wrong proof if you know that the theorem is wrong: You just pick an example where the theorem fails, and see what the proof is saying about that example. The simplest example where our present theorem fails is the case $n = 2$. This is the very smallest instance of our induction step. So something must be wrong in the induction step for $n = 1$ (since the theorem is true for 1 horse and false for 2 horses). Here, we are arguing that the first horse H_1 and the last horse $H_{n+1} = H_2$ have the same color as the "middle horses" $H_2, H_3, \ldots, H_1$. But there are no middle horses, so it makes no sense to compare colors with them. In particular, we cannot conclude that H_1 and H_2 have the same color.

The mistake we made is really a logical mistake: Normally, $a = b$ and $b = c$ implies $a = c$. But $a = b_1 = b_2 = \cdots = b_n$ and $c = b_1 = b_2 = \cdots = b_n$ does not imply $a = c$ when $n = 0$.

□

Let me stress how one simple mistake has brought down the whole proof. The induction step would work for all $n \neq 1$. For an induction proof to work, the implication $P(n) \Longrightarrow P(n+1)$ must be proved for **every** n. If it fails for a single n, the whole chain breaks down. For example, if we have a statement $P(n)$ for each $n \geq 0$, and we have proved the base case $P(0)$ and the implication $P(n) \Longrightarrow P(n+1)$ for all $n \neq 4$, then we can conclude that $P(0)$, $P(1)$, $P(2)$, $P(3)$, $P(4)$ hold, but we cannot guarantee any of $P(5)$, $P(6)$, $P(7)$, ...

1.8. More on the Fibonacci numbers

Recall the Fibonacci sequence $(f_0, f_1, f_2, \ldots)$, given by

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

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 further properties of this sequence now.

1.8.1. The addition theorem

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

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

Proof. Can we induct on two variables at the same time? Yes, if you "nest" one induction in the other, but we'd rather not do it.

It is better to pick one variable and induct on it, when that works. Let us induct on n. To that purpose, for every integer $n \geq 0$, we define the statement $P(n)$ to say

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

(Don't forget the "for every integer $m \geq 0$" part here! If we only stated $P(n)$ for a single value of m, then the induction step below would not work.)

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

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

$$\text{"for every integer } m \geq 0, \text{ we have } f_{0+m+1} = f_{0+1}f_{m+1} + f_0 f_m\text{"}.$$

But this is true, since

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

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

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

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

In other words,

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

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

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

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

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

But our induction hypothesis says that

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

We can apply this to $p = m+1$. Thus, we obtain

$$f_{n+m+1+1} = f_{n+1} f_{m+1+1} + f_n f_{m+1} = f_{n+1} f_{m+2} + f_n f_{m+1}.$$

Comparing this with

$$f_{n+1+1} f_{m+1} + f_{n+1} f_m = f_{n+1} f_{m+2} + f_n f_{m+1},$$

we find

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

In other words,

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

This completes the induction step, and so the theorem is proved. □

See HW1 for more about the Fibonacci sequence and a generalization of the above theorem to more general recursive sequences.

1.8.2. Divisibility of Fibonacci numbers

Our next theorem involves divisibility of integers. We will study this in detail in a later chapter (§3.1), but for now let me just show the 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 in this case.

For example, we have $2 \mid 4$ and $3 \mid 12$ and $10 \mid 30$ and $0 \mid 0$ and $5 \mid 0$, but we don't have $2 \mid 3$ or $0 \mid 1$.

Now we have the following property of Fibonacci numbers:

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

For example, $3 \mid 9$ implies $f_3 \mid f_9$, which is true ($f_3 = 2$ and $f_9 = 34$).
For another example, $6 \mid 12$ implies $f_6 \mid f_{12}$, which is true as well.

Proof of the theorem. It is reasonable to try induction. Alas, inducting on a does not work, since the condition $a \mid b$ in the induction hypothesis is completely unrelated to the condition $a+1 \mid b$ in the induction step. Inducting on b suffers from the same problem, since the conditions $a \mid b$ and $a \mid b+1$ are also fairly unrelated.

So we should induct on something else. On what? On a new variable we introduce. Namely, recall that $a \mid b$ means "$b = ac$ for some integer c". Moreover, for $a, b \geq 0$ we can pick $c \geq 0$. So we can restate our theorem as follows:

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

We shall now 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 $P(0)$. This is saying 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 every integer. So the base case is done.

Induction step: Let $c \geq 0$ be any integer. We 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 statement $P(c)$) shows that $f_a \mid f_{ac}$. In other words, $f_{ac} = f_a \cdot p$ for some integer p. Consider this p. Now,

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

Thus, $f_a \mid f_{a(c+1)}$. Thus, we have shown that for any integer $a \geq 0$, we have $f_a \mid f_{a(c+1)}$. In other words, we have proved $P(c+1)$. This completes our induction step, and thus the proof.

Right?

I claim that there is a minor but nontrivial mistake in the above proof. Again, our use of induction is not the problem. Recall the addition theorem: It says that

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

We have applied this theorem to $n = ac$ and $m = a-1$. Is this allowed? Not if $a = 0$, because in this case $m = a-1 = 0-1 = -1$ is not ≥ 0. Fortunately, this problem occurs only in the $a = 0$ case, and this case is trivial (since $f_a \mid f_{ac}$ for $a = 0$ is just saying that $f_0 \mid f_0$, which is obvious). Nevertheless, strictly speaking, this case needs to be accounted for. So we have to replace our above induction step by the following:

Induction step (corrected): Let $c \geq 0$ be any integer. We 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 statement $P(c)$) shows that $f_a \mid f_{ac}$. In other words, $f_{ac} = f_a \cdot p$ for some integer p. Consider this p.

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, $a = 0$. Hence, $a(c+1) = 0(c+1) = 0$. Thus, $f_a \mid f_{a(c+1)}$ (since $f_a = f_0$ and $f_{a(c+1)} = f_0$ are just the same number). Thus, our goal (to prove $f_a \mid f_{a(c+1)}$) is achieved in Case 1.

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

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

Thus, $f_a \mid f_{a(c+1)}$. Thus, we have shown that for any integer $a \geq 0$, we have $f_a \mid f_{a(c+1)}$. So we have proved $f_a \mid f_{a(c+1)}$ in Case 2.

Now, our goal (showing that $f_a \mid f_{a(c+1)}$) is reached in both Case 1 and Case 2. The induction step is therefore complete. $\square$

1.8.3. Binet's formula

Is there an explicit formula for f_n, that is, a formula that computes f_n directly, without requiring the previous entries?

Yes, known as **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:

- Why on earth would you expect a formula for the Fibonacci numbers (integers!) to include irrational numbers like φ and ψ ?

  (Eigenvalues of matrices provide an explanation, but it will remain a mystery for this course. Just one hint: φ and ψ are the roots of the quadratic equation $x^2 = x + 1$, which is "similar" to the Fibonacci recurrence $f_n = f_{n-1} + f_{n-2}$.)

- Binet's formula can be used to compute $f_{1\ 000\ 000}$ for example reasonably fast.

- As n grows large, ψ^n approaches 0 whereas φ^n grows exponentially. Hence, f_n grows exponentially as well (by Binet's formula), with growth rate $\varphi \approx 1.618\ldots$.

- The number φ is known as the **golden ratio**. The number ψ is known as its conjugate.

Proof of Binet's formula, first attempt. We induct on n.

Base case: For $n = 0$, the formula says that $f_0 = \dfrac{\varphi^0 - \psi^0}{\sqrt{5}}$, which is indeed true since both sides are 0.

Induction step: Fix an integer $n \geq 0$. Assume (as the IH) that the theorem holds for n, i.e., that we have $f_n = \dfrac{\varphi^n - \psi^n}{\sqrt{5}}$.

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

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

For $n = 0$, this is easy. For $n \geq 1$, we have

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

We are stuck here, since the IH tells us nothing about f_{n-1}. Metaphorically, the n-th domino is not strong enough to kick over the $(n+1)$-st domino; the induction step does not work.

Next time, we will see how to "strengthen" the induction principle to make it work for this theorem. ($\Longrightarrow$ strong induction) $\square$

1.9. Strong induction

1.9.1. Reminder on regular induction

Recall the original principle of induction:

Theorem 1.9.1 (Principle of Induction)**.** Let b be an integer. Let $P(n)$ be a statement defined for each integer $n \geq b$. 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 principle a bit by renaming the n in the induction step as $n-1$ (so that the implication $P(n) \Longrightarrow P(n+1)$ becomes $P(n-1) \Longrightarrow P(n)$). So it takes the following form:

Theorem 1.9.2 (Principle of Induction, restated)**.** Let b be an integer. Let $P(n)$ be a statement defined for each integer $n \geq b$. 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 this principle (in either form) is that the base case gives us $P(b)$ whereas the induction step gives us the implications

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

and we can climb this "ladder" to reach any $P(n)$ for any $n \geq b$. In the domino metaphor, this is saying that each $P(n)$ domino is kicked over by the $P(n-1)$ domino.

1.9.2. Strong induction

Now imagine that $P(n-1)$ alone is not sufficient to topple $P(n)$, but the combined momentum of the first dominos $P(b)$, $P(b+1)$, $\ldots$, $P(n-1)$ is. In other words, imagine that we prove the implications

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

This would still be enough to yield $P(n)$ for all $n \geq b$.

This induction principle is known as **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 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 each integer $n \geq b$.

Proofs using this principle are called **proofs by strong induction** (or **strong induction proofs**). They differ from proofs by (regular) induction in that in the induction step, instead of assuming $P(n-1)$ as the induction hypothesis, you assume the conjunction

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

as the induction hypothesis. This gives you a lot more to work with.

(We will later see a slightly nicer form of strong induction, which doesn't even require a base case.)

Before we see a proof using strong induction, let me explain why it works:

Let us say you have proved a statement $P(n)$ for all $n \geq 0$ by strong induction. Thus:

- In the base case, you have proved $P(0)$.
- The induction step yields $P(0) \implies P(1)$. Thus, you get $P(1)$ (since you have $P(0)$).
- The induction step yields $(P(0) \text{ AND } P(1)) \implies P(2)$. Thus, you get $P(2)$ (since you have $P(0)$ and $P(1)$).
- The induction step yields $(P(0) \text{ AND } P(1) \text{ AND } P(2)) \implies P(3)$. Thus, you get $P(3)$ (since you have $P(0)$ and $P(1)$ and $P(2)$).
- And so on.

Actually, the strong induction principle can be derived from the regular induction principle by a simple trick (see references in the notes).

1.9.3. Example: Proof of Binet's formula

Let us now prove Binet's formula by strong induction:

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

Base case: Same as before: We check that the theorem holds for $n = 0$.

Induction step: Let $n > 0$ be an integer. Assume (as the induction hypothesis) that Binet's formula holds for 0, for 1, for 2, ..., for $n-1$ instead of n. In other words, we assume that

$$f_k = \frac{\varphi^k - \psi^k}{\sqrt{5}} \qquad \text{for each } k \in \{0, 1, \ldots, n-1\}.$$

Now we must prove that Binet's formula holds for n. In other words, we must prove that $f_n = \dfrac{\varphi^n - \psi^n}{\sqrt{5}}$.

If $n = 1$, then this is easy to check directly. ($f_1 = 1$ and $\dfrac{\varphi^1 - \psi^1}{\sqrt{5}} = \dfrac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} = 1$). So from now on, we assume that $n \neq 1$. Hence, $n \geq 2$.

The recursive definition of the Fibonacci sequence yields

$$f_n = f_{n-1} + f_{n-2} = \frac{\varphi^{n-1} - \psi^{n-1}}{\sqrt{5}} + \frac{\varphi^{n-2} - \psi^{n-2}}{\sqrt{5}}$$

(since we can apply our induction hypothesis to $k = n-1$, obtaining $f_{n-1} = \frac{\varphi^{n-1} - \psi^{n-1}}{\sqrt{5}}$, and also to $k = n-2$, obtaining $f_{n-2} = \frac{\varphi^{n-2} - \psi^{n-2}}{\sqrt{5}}$). Thus,

$$\begin{aligned} f_n &= \frac{\varphi^{n-1} - \psi^{n-1}}{\sqrt{5}} + \frac{\varphi^{n-2} - \psi^{n-2}}{\sqrt{5}} \\ &= \frac{1}{\sqrt{5}} \underbrace{\left(\varphi^{n-1} + \varphi^{n-2}\right)}_{\substack{=\varphi^{n-2}(\varphi+1) \\ =\varphi^{n-2}\varphi^2 \\ =\varphi^n \\ \text{(the equality } \varphi+1=\varphi^2 \\ \text{can be checked directly)}}} - \frac{1}{\sqrt{5}} \underbrace{\left(\psi^{n-1} + \psi^{n-2}\right)}_{\substack{=\psi^{n-2}(\psi+1) \\ =\psi^{n-2}\psi^2 \\ =\psi^n \\ \text{(similarly)}}} \\ &= \frac{1}{\sqrt{5}}\varphi^n - \frac{1}{\sqrt{5}}\psi^n = \frac{\varphi^n - \psi^n}{\sqrt{5}}. \end{aligned}$$

In other words, Binet's formula holds for n. This completes the induction step. □

To recap: We were able to prove Binet's formula using strong induction but not using regular induction, since the recursive equation $f_n = f_{n-1} + f_{n-2}$ referenced the **two** previous entries of the Fibonacci sequence (rather than only the single one f_{n-1}), and we needed to have an induction hypothesis that tells us something about both of them (not just about f_{n-1}). In other words, we needed an induction that has a longer memory than just "the statement for $n-1$". Strong induction does the trick.

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 proved manually because we could not go down to $n-2$ when $n = 1$. In the domino metaphor, if each domino is kicked over by the previous two, then we have to kick over the first two dominos by hand.

1.9.4. Baseless strong induction

You can actually reformulate the principle of strong induction in a form that does not have 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 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 each integer $n \geq b$.

How does this restated principle do its job without a base case? Easy: We have just repackaged the base case into the induction step. Indeed, the induction step now says "$n \geq b$" instead of "$n > b$", so that it includes the $n = b$ case. In the $n = b$ case, the implication

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

says

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

i.e., it says that $P(b)$ is unconditionally true. But this is precisely what the base case would be proving.

We have thus not magically removed the need for a base case; we just have folded it into the induction step. This new version of strong induction is slightly cleaner, but in practice its use often boils down to the same thing.

1.9.5. Example: Prime factorizations exist

Another example of a strong induction proof comes from elementary number theory. We recall:

Definition 1.9.5. A **prime** (or **prime number**) means an integer $p > 1$ whose only positive divisors are 1 and p. (A **divisor** of an integer b means an integer a such that $a \mid b$.)

So the primes (in increasing order) are

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

There are infinitely many of them, as you are going to show some time soon.

Theorem 1.9.6. 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.
- $2025 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5$ is a product of six primes.
- $2 = 2$ is a product of one prime (itself).

How do we prove the theorem in general?

Proof. 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 (of 0 primes, as we saw).

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

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

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

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

We are in one of the following two cases:

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

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

Consider Case 1 first. In this case, n itself is a prime (by the definition of a prime), and thus is a product of finitely many primes (namely, of 1 prime). So $P(n)$ 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), but we take this for granted). Hence, $1 < d < n$ (since d is neither 1 nor n). This shows that d is one of the numbers $1, 2, \ldots, n-1$. Therefore, $P(d)$ holds (since we assumed that $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(n-1)$ holds). In other words, d is a product of finitely many primes. Thus, 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 primes $p_1, p_2, \ldots, p_k$.

Since d is a divisor of n, the fraction $\dfrac{n}{d}$ is an integer. Moreover, this integer $\dfrac{n}{d}$ is positive (since d and n are positive) and is $< n$ (since $d > 1$). Hence, $\dfrac{n}{d}$ is one of the numbers $1, 2, \ldots, n-1$. Hence, $P\left(\dfrac{n}{d}\right)$ holds (since we assumed

that $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(n-1)$ holds). In other words, $\dfrac{n}{d}$ is a product of finitely many primes. Thus, we can write $\dfrac{n}{d}$ 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 primes $q_1, q_2, \ldots, q_\ell$.

Now,

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

Hence, n is a product of finitely many primes. In other words, $P(n)$ is true. Thus, the induction step is complete, and the theorem is proved. □

The above proof just formalizes the standard method of factoring a positive integer n into a product of prime: We search for a positive divisor d that is neither 1 nor n. If such a d does not exist, then n itself is a prime. If it does, then we are reduced to the simpler problems of factoring d and $\dfrac{n}{d}$, and just need to multiply the resulting factorizations.

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

Here is another example of how to use 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 using these coins?

Let's make a table:

0 cents	yes
1 cents	no
2 cents	no
3 cents	yes
4 cents	no
5 cents	yes
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.

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

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 1.9.7. 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 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.

Since $n > 8$, we are in one of the following three cases:

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 $n = 9 = 3 \cdot 3 + 0 \cdot 5$ (that is, n cents can be paid with three 3-cent coins).

In Case 2, we are done, since $n = 10 = 0 \cdot 3 + 2 \cdot 5$ (that is, n cents can be paid with two 5-cent coins).

Now consider Case 3. In this case, $n \geq 11$. Hence, $n - 3 \geq 8$. This yields that $n - 3$ is one of the numbers $8, 9, \ldots, n-1$. Hence, the induction hypothesis (applied to $n - 3$) yields that $n - 3$ can be paid with 3-cent and 5-cent coins, i.e., that we can write $n - 3$ as $n - 3 = 3c + 5d$ with $c, d \in \mathbb{N}$. Using these $c, d \in \mathbb{N}$, we therefore have

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

which shows that n cents can also be paid with 3-cent and 5-cent coins. This shows that the proposition is true for n, and thus we are done. □

Note that the above proof had one "de-jure base case" (the case $n = 8$) but also two "de-facto base cases" (the cases $n = 9$ and $n = 10$, which were formally part of the induction step but still had to be treated by hand because we could not apply the induction hypothesis to $n - 3$ in those cases).

2. Sums and products

2.1. Finite sums

Previously, we have encountered sums such as

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

Such sums can be tricky to decipher: What exactly does the "$\cdots$" mean? This is not a good notation when sums get more complicated, and certainly not a rigorous notation. So let us introduce a rigorous one:

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 defined to be 0.

The above notation is called **sum notation** or **sigma notation**.

Examples:

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

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

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

$$\sum_{k=6}^{11} 3 = 3+3+3+3+3+3 = 18;$$

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

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

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

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

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

Thus, our theorem from a few classes ago can be restated as follows:

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 variable (as long as it doesn't have a different meaning already). For instance, you can rewrite $\sum_{k=u}^{v} a_k$ as $\sum_{i=u}^{v} a_i$ or $\sum_{x=u}^{v} a_x$ or $\sum_{\bigstar=u}^{v} a_\bigstar$ or whatnot. But don't write $\sum_{u=u}^{v} a_u$.

[The summation sign has much in common with the integral sign; you can think of $\sum_{k=u}^{v} a_k$ as a discrete analogue of $\int_u^v f(x)\,dx$. There are some differences:

For example, $\int_u^u f(x)\,dx = 0$ whereas $\sum_{k=u}^{u} a_k = a_u$. Also, $\int_u^{u-1} f(x)\,dx \neq 0$ usually but $\sum_{k=u}^{u-1} a_k = 0$.

In Python, $\sum_{k=u}^{v} a_k$ is written `sum(a(k) for k in range(u, v+1))`.]

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

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

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

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

$$\sum_{k=1}^{n} (2k-1) = 1 + 3 + 5 + 7 + \cdots + (2n-1)$$
$$= (\text{the sum of the first } n \text{ odd positive integers}).$$

Let us actually 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, if you rewrite this without sigma notation, you see it become
$$(a_u - b_u) + (a_{u+1} - b_{u+1}) + \cdots + (a_v - b_v)$$
$$= (a_u + a_{u+1} + \cdots + a_v) - (b_u + b_{u+1} + \cdots + b_v).$$

- 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 tell whether something is a valid rule by rewriting it without sigma notation.

Let us now compute the last sum we wrote down:

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

See the whiteboard for a different, "geometric" proof of this equality. We will see (towards the end of this course) a combinatorial formalization of this proof.

As another illustration of finite sum notation and its uses, let us rewrite Gauss's proof of the Little Gauss formula

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

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

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

- We have
$$\sum_{k=u}^{v} a_k = \sum_{k=u}^{v} a_{u+v-k}$$
for any integers u, v and any numbers a_k. Indeed, restating this without finite sum notation, it takes the form
$$a_u + a_{u+1} + \cdots + a_v = a_v + a_{v-1} + \cdots + a_u,$$
which is just saying that a finite sum does not change if you write it in reverse. This rule is called "substituting $u+v-k$ for k in the sum" or "turning the sum upside down" or "reversing the sum".

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

Now, Gauss's proof of his formula looks as follows:

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

so $\sum\limits_{k=1}^{n} k = \dfrac{n \cdot (n+1)}{2}$, qed.

We have now found closed-form expressions (i.e., expressions with no $\sum$ signs or "$\cdots$"s) for several sums. Not every sum has such an expression. For example, $\sum\limits_{k=1}^{n} \dfrac{1}{k}$ cannot be simplified; neither can $\sum\limits_{k=1}^{n} k^k$.

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.

Here are two more rules for finite sums:

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

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

  This is very useful for induction proofs.

- More generally, any 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 the summation sign, this would say

$$\begin{aligned} &a_u + a_{u+1} + \cdots + a_v \\ &= (a_u + a_{u+1} + \cdots + a_w) + (a_{w+1} + a_{w+2} + \cdots + a_v)\,. \end{aligned}$$

Finite sum notation can be extended somewhat. For example, using some common sense, you should be able to guess that

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

where m is the largest even element of $\{1, 2, \ldots, n\}$. See the references in the notes for a more detailed explanation of this notation.

See also the notes (end of §2.1) for a bunch of exercises, some of which will be on the HW.

2.2. Finite products

Finite products are the analogue of finite sums using multiplication instead of addition.

Theorem 2.2.1. Let u and v be two integers. Let $a_u, a_{u+1}, \ldots, a_v$ be any 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 $v < u$, this product is called **empty** and defined to be 1.

For example:

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

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

$$\prod_{k=1}^{n} a = \underbrace{aa \cdots a}_{n \text{ times}} = a^n \qquad \text{(for any number } a\text{)};$$

$$\prod_{k=1}^{n} a^k = a^1 a^2 \cdots a^n = a^{1+2+\cdots+n} = a^{n(n+1)/2} \qquad \text{(for any number } a\text{)}.$$

In a finite product $\prod_{k=u}^{v} a_k$, 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 terminology for sums. Let me only state the "splitting-off" rule for products:

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

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

  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**") to be

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

This is the product of the first n positive integers.

For example,

$$6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720.$$

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

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

Proof. We have

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

□

Six exercises on factorials and products can be found in §2.3 of the notes.

2.4. Binomial coefficients: Definition

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

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

- If $k \in \mathbb{N}$, then we set
$$\binom{n}{k} := \frac{n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right)}{k!}$$
(where is the numerator is the product of k consecutive "integers", the largest of which is n; you can also write it as $\prod_{i=0}^{k-1}\left(n-i\right)$).
- If $k \notin \mathbb{N}$, then we set
$$\binom{n}{k} := 0.$$

The number $\binom{n}{k}$ is called the **binomial coefficient** of n and k (and is pronounced "n choose k"). Do not mistake it for a vector.

Example 2.4.2. For any number n, we have
$$\begin{aligned}
\binom{n}{3} &= \frac{n\left(n-1\right)\left(n-2\right)}{3!} = \frac{n\left(n-1\right)\left(n-2\right)}{6}; \\
\binom{n}{2} &= \frac{n\left(n-1\right)}{2}; \\
\binom{n}{1} &= \frac{n}{1} = n; \\
\binom{n}{0} &= \frac{\left(\text{empty product}\right)}{0!} = \frac{1}{1} = 1; \\
\binom{n}{2.5} &= 0 \qquad \left(\text{since } 2.5 \notin \mathbb{N}\right); \\
\binom{n}{-1} &= 0 \qquad \left(\text{since } -1 \notin \mathbb{N}\right).
\end{aligned}$$

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

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

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

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 pattern we spot here is the following:

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

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

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

since one of the factors in the numerator is $n - n = 0$. Thus, $\binom{n}{k} = 0$.

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

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

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

The above proposition explains why our table has so many 0's. So a better way to tabulate the binomial coefficients (at least the ones of the form $\binom{n}{k}$ with $n, k \in \mathbb{N}$) is as follows:

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

This is known as **Pascal's triangle** and has many wondrous properties. In particular, we observe:

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

We shall now prove all of these and more.

2.5. Binomial coefficients: Properties

We begin with the most important property of BCs (= binomial coefficients):

Theorem 2.5.1 (Pascal's identity)**.** For any numbers n and k, we have

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

For example, for $n = 7$ and $k = 3$, this is saying that $\binom{7}{3} = \binom{6}{2} + \binom{6}{3}$. Explicitly, this is saying that $35 = 15 + 20$.

But the theorem also holds for non-integer or negative n's and k's.

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

Case 1: The number k is a positive integer.

Case 2: We have $k = 0$.

Case 3: None of the above.

Let us first consider Case 1. Here, k is a positive integer, so that both k and $k-1$ belong to $\mathbb{N}$. Thus, the definition of BCs yields

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

Setting $a := (n-1)\,(n-2)\cdots(n-k+1)$, we can simplify these equalities to

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

But the claim that we are trying to prove is

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

Using the above three equalities, this can be rewritten as

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

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 $k! = (k-1)! \cdot k$), this simplifies to

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

which is clearly true. Thus, our claim is proved in Case 1.

Let us next consider Case 2. In this case, $k = 0$. Our claim

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

thus 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 true.

Finally, consider Case 3. In this case, $k \notin \mathbb{N}$. Hence, $k-1 \notin \mathbb{N}$. Thus, our claim

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

is clearly true.

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

2.5.1. The factorial formula

Binomial coefficients $\binom{n}{k}$ make sense for arbitrary numbers n and k. However, in the particular case when $n \in \mathbb{N}$ and $k \in \{0, 1, \ldots, n\}$ (this is the case that Pascal's triangle shows), there is a particularly simple formula for $\binom{n}{k}$:

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 $\binom{n}{k}$ yields

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

So

$$\begin{aligned} k! \cdot \binom{n}{k} &= n\,(n-1)\,(n-2)\cdots(n-k+1) \\ &= (n-k+1)\,(n-k+2)\,(n-k+3)\cdots n \\ &= \frac{1\cdot 2\cdot\cdots\cdot n}{1\cdot 2\cdot\cdots\cdot(n-k)} \qquad \left(\begin{array}{c}\text{here, we added new}\\ \text{factors to our product,}\\ \text{only to divide them back out}\end{array}\right) \\ &= \frac{n!}{(n-k)!}. \end{aligned}$$

Dividing by $k!$, we transform this into

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

□

Corollary 2.5.3. For any $n \in \mathbb{N}$, we have $\binom{n}{n} = 1$.

Proof. By the factorial formula,

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

□

Warning: Neither the theorem nor the corollary holds if we don't require what we required (that is, $n \in \mathbb{N}$ in both cases, and $k \in \{0,1,\ldots,n\}$ for the theorem). For example, $\binom{-1}{-1} = 0$, not 1. So if you want to compute $\binom{1.7}{3}$, you have to use the definition, not the factorial formula.

2.5.2. The symmetry of binomial coefficients

Theorem 2.5.4 (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.

Consider Case 1. We have $k \in \{0, 1, \ldots, n\}$, so that $n - k \in \{0, 1, \ldots, n\}$. Thus, by the factorial formula,

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

which are the same number. So the theorem is proved in Case 1.

Now consider Case 2. Here we have $k < 0$. Hence, $k \notin \mathbb{N}$ and thus $\binom{n}{k} = 0$ by definition. However, $n - k > n$ (since $k < 0$), so that $\binom{n}{n-k} = 0$ (by our first proposition on BCs). So we must prove $0 = 0$, which is obvious.

Case 3 is similar to Case 2 (it's the same case with the roles of k and $n - k$ swapped).

Case 4 is trivial ($0 = 0$). □

Warning: The symmetry of BCs does not hold for negative (or non-integer) n.

2.5.3. Pascal's triangle consists of integers

We defined $\binom{n}{k}$ as a fraction, and yet:

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

Proof. We induct on n.

Base case: The theorem holds for $n = 0$, since

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

Induction step: We make our induction step from $n - 1$ to n (instead of, as usual, 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 also holds for n. In other words, we must prove that

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

But 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, and the theorem is proved. □

Wouldn't it be nicer to have a more explanatory proof of the theorem, rather than just an induction proof that tells you that the theorem is true? Such a proof indeed exists:

Theorem 2.5.6 (combinatorial interpretation of BCs)**.** Let $n \in \mathbb{N}$, and let k be a number. Let A be any n-element set (i.e., a set with n elements, such as $\{1, 2, \ldots, n\}$). 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

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

So there are 6 of them. This agrees with the theorem, since $\binom{4}{2} = 6$.

We will prove the theorem later on (Chapter 4), as we learn more about finite sets and counting. Note that it explains the word "choose" in "n choose k".

The theorem implies that $\binom{n}{k} \in \mathbb{N}$ for all $n \in \mathbb{N}$ and all numbers k. Of course, it does not say anything about negative or non-integer n's.

2.5.4. Upper negation

Theorem 2.5.8 (upper negation formula)**.** For any numbers n and $k \in \mathbb{Z}$, we have

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

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

So let us consider the case when $k \in \mathbb{N}$. 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 equalities, 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 $\binom{n}{k} \in \mathbb{Z}$.

Proof. If $n \geq 0$, then this has already been proved above.

If $k \notin \mathbb{N}$, then this is clear since $\binom{n}{k} = 0$.

In the remaining case, use the upper negation formula. Details left to the reader. □

2.5.5. 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

$$f_8 = 1 + 6 + 10 + 4 + 0 + 0 + 0 = 21.$$

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

2.6. The binomial formula

The reason why BCs are called BCs is the **binomial formula**:

Theorem 2.6.1 (binomial formula, aka binomial theorem)**.** Let a and b be any 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

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

Similarly, for $n = 2$, this says

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

Proof of the binomial formula. It suffices to prove the first formula, i.e.,

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

To prove this, we induct on n.

Base case: For $n = 0$, this formula is saying that $(a+b)^0 = \sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k}$, which boils down to $1 = 1$.

Induction step: Let $n \in \mathbb{N}$. We assume (as the IH) that the formula 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 now prove that it also holds for $n+1$, i.e., that we have

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

Indeed, we have

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

On the other hand,

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

So we need to prove that

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

Part of this is easy: We have

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

because $n-k+1 = n+1-k$ and because the only addend on the RHS that is missing from the LHS is $\underbrace{\binom{n}{n+1}}_{\substack{=0 \\ \text{(since } n+1>n\text{)}}} a^{n+1} b^{n+1-(n+1)} = 0$.

Remains the other part: We must prove that

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

The sum on the RHS starts at $k = 0$, but its very first addend (the $k = 0$) addend is $\underbrace{\binom{n}{-1}}_{=0} a^0 b^{n+1-0} = 0$, so that we can just as well have it start at $k = 1$. So we must prove 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 these sums are equal, because both of them are

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

More formally, this argument is an instance of an important summation rule known as **substitution**. In its simplest form, this rule says that

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

for any integers u, v, δ and any numbers $c_u, c_{u+1}, \ldots, c_v$. This is the discrete analogue of the 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 of the form $\sum_{k=u}^{v} c_k$ as $\sum_{k=u+\delta}^{v+\delta} c_{k-\delta}$, we say that we are **substituting** $k-\delta$ for k in the sum. Thus, substituting $k-1$ for k in the sum $\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k}$, we obtain

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

which is exactly the formula that we needed.

Altogether, we now have

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

This means that the binomial formula holds for $n+1$. This completes the induction step and, with it, the proof. □

Corollary 2.6.3. Let $n \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n}\binom{n}{k} = 2^n.$$

Proof. We have

$$\begin{aligned}2^n = (1+1)^n &= \sum_{k=0}^{n}\binom{n}{k}\underbrace{1^k 1^{n-k}}_{=1} \qquad \text{(by the binomial formula)} \\ &= \sum_{k=0}^{n}\binom{n}{k}.\end{aligned}$$

□

3. Elementary number theory

Number theory means the study of integers and similar objects. Crucial roles are played by divisibility and by prime numbers.

3.1. Divisibility

3.1.1. Definition

We begin by defining the most important concept in number theory:

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 $4 \nmid 11$, because there is no integer c such that $11 = 4c$.
(c) We have $1 \mid b$ for every integer b, since $b = 1 \cdot b$.
(d) We have $a \mid a$ for every integer a, since $a = a \cdot 1$. In particular, $0 \mid 0$.
(e) We have $a \mid 0$ for every integer a, since $0 = a \cdot 0$.
(f) An integer b satisfies $0 \mid b$ if and only if $b = 0$.

The well-known concepts of even and odd integers are particular cases:

Definition 3.1.3. **(a)** An integer n is **even** if $2 \mid n$.
(b) An integer n is **odd** if $2 \nmid n$.

You probably know that

1. the sum of two even integers is even;
2. an even plus an odd integer is odd;
3. the sum of two odd integers is even.

The first claim here is obvious ($2a + 2b = 2(a + b)$), but the third claim is not. We need to understand divisibility better to prove it.

3.1.2. Basic properties

Let me use the notation $\operatorname{abs} x$ for the absolute value $|x|$ where $x \in \mathbb{R}$.

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 is just saying that the divisibility $a \mid b$ does not depend on the signs of a and b. In other words, it says that we can replace a and b by $\operatorname{abs} a$ and $\operatorname{abs} b$ without changing this divisibility.

To prove this, it suffices to show the following two claims:

1. If $a \mid b$, then $-a \mid b$.
2. If $a \mid b$, then $a \mid -b$.

Claim 1 is easy: If $a \mid b$, then $b = ac$ for some integer c, and therefore $b = ac = (-a)(-c)$, so that $-a \mid b$.

Claim 2 is also easy: If $a \mid b$, then $b = ac$ for some integer c, and therefore $-b = -ac = a(-c)$, so that $a \mid -b$.

Having proved Claims 1 and 2, we see that the divisibility $a \mid b$ does not become false if we flip the sign of a or of b. Thus, it does not become true either (since in that case, by flipping the sign again, we could recover $a \mid b$).

So $a \mid b$ does not depend on the signs of a and b, and we have proved part **(a)**.

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

Set $x = \operatorname{abs} a$ and $y = \operatorname{abs} b$. Then, from $a \mid b$, we obtain $x \mid y$ (by part **(a)**). Hence, $y = xz$ for some integer z. Consider this z.

From $b \neq 0$, we get $y > 0$, so $xz = y > 0$. Hence, $z > 0$ (since $x \geq 0$). Therefore, $z \geq 1$ (since z is an integer). Now,

$$y = xz = \underbrace{x}_{\geq 0} \underbrace{(z-1)}_{\substack{\geq 0 \\ (\text{since } z \geq 1)}} + x \geq x.$$

In other words, $\operatorname{abs} b \geq \operatorname{abs} a$. Equivalently, $\operatorname{abs} a \leq \operatorname{abs} b$. This proves part **(b)**.

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

If $a = 0$, then this is easy (since $a = 0$ and $a \mid b$ easily implies $b = 0$).

If $b = 0$, then this is also easy (for the same reason).

Now consider the case when neither a nor b is 0. Hence, part **(b)** of our proposition yields $\operatorname{abs} a \leq \operatorname{abs} b$. But the same reasoning (with a and b trading roles) yields $\operatorname{abs} b \leq \operatorname{abs} a$. Combining these inequalities, we obtain $\operatorname{abs} a = \operatorname{abs} b$. So part **(c)** is proved.

(d) Assume that $a \mid b$. Then, $b = ac$ for some integer c. This integer c must then satisfy $c = \dfrac{b}{a}$ (since $b = ac$ and $a \neq 0$). Therefore, $\dfrac{b}{a} = c \in \mathbb{Z}$.

Conversely, if $\dfrac{b}{a} \in \mathbb{Z}$, then $b = ac$ for some integer c (namely, for $c = \dfrac{b}{a}$).

So each of the two statements $a \mid b$ and $\dfrac{b}{a} \in \mathbb{Z}$ implies the other. This proves that they are equivalent. $\square$

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 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 a multiple of d.)

Proof. **(a)** We have $a = a \cdot 1$.

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

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

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

Consider these x and y.

We have

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

Therefore, there exists an integer z such that $c = az$ (namely, $z = xy$). In other words, $a \mid c$.

(c) Let a_1, a_2, b_1, b_2 satisfy $a_1 \mid b_1$ and $a_2 \mid b_2$.

Since $a_1 \mid b_1$, there exists an integer c_1 such that $b_1 = a_1 c_1$.

Since $a_2 \mid b_2$, there exists an integer c_2 such that $b_2 = a_2 c_2$.

Consider these c_1 and c_2. Now,

$$b_1 b_2 = (a_1 c_1)(a_2 c_2) = (a_1 a_2)(c_1 c_2).$$

This shows that $a_1 a_2 \mid b_1 b_2$ (since $c_1 c_2$ is an integer).

(d) Let $d, a, b \in \mathbb{Z}$ satisfy $d \mid a$ and $d \mid b$.

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

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

Consider these x and y. Now,

$$a + b = dx + dy = d(x + y).$$

This shows that $d \mid a + b$. □

Part **(b)** of the above theorem allows us to chain divisibilities together. Correspondingly, two statements of the form $a \mid b$ and $b \mid c$ are commonly written together as "$a \mid b \mid c$", and automatically imply $a \mid c$. Likewise, 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), and such a chain of divisibilities automatically entails $a_1 \mid a_k$ (this is proved by induction on k). For instance, $3 \mid 6 \mid 18$.

Exercise 3.1.1. Let $a, b \in \mathbb{Z}$ satisfy $a \mid b$. 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, there is a bunch of known **divisibility criteria** that characterize the integers divisible by a. Here are some:

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. Is the number 25473 divisible by 3 ? Its sum of digits is $2+5+4+7+3 = 21$ is divisible by 3, so (by part **(d)** above) the number 25473 is divisible by 3 as well.
Is it divisible by 9 ? No (by part **(e)** above), since 21 is not divisible by 9.

How would you prove the above theorem?
Part **(c)** is easy:

- If $10 \mid b$, then the last digit of b is 0 because multiplying an integer by 10 simply inserts a 0 at its end.
- If the last digit of b is 0, then $b = 10b'$, where b' is b without its last digit.

Parts **(a)** and **(b)** are somewhat trickier, and parts **(d)** and **(e)** significantly so. To find simple proofs for them, we now introduce another relation between integers: **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 "$a \not\equiv b \bmod n$".

(LaTeX: "a \equiv b \mod n".)

Example 3.2.2. **(a)** Is $3 \equiv 7 \bmod 2$? Yes, since $2 \mid 3-7$ (because $3-7=-4=2\cdot(-2)$).
(b) Is $3 \equiv 6 \bmod 2$? No, since $2 \nmid 3-6$.
(c) We have $a \equiv b \bmod 1$ for any integers a and b. This is because $1 \mid a-b$.
(d) Two integers a and b satisfy $a \equiv b \bmod 0$ if and only if $a=b$.
(e) For any integers a and b, we have $a+b \equiv a-b \bmod 2$, since $(a+b)-(a-b)=2b$ is a multiple of 2.

The word "modulo" means something like "with respect to" or "as seen by". The statement "a is congruent to b modulo n" can be rewritten as "a equals b up to a multiple of n", because we have

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

What does it mean for two integers a and b to be congruent modulo 2 ? It means that they are either both even or both odd (i.e., they have the same parity). Strictly speaking, we don't know this yet; we will prove this in the next section.

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, we have

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

□

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

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

then

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

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

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

Proof. **(a)** For every $a \in \mathbb{Z}$, we have $n \mid a - a$ (since $a - a = 0 = n \cdot 0$). Thus, $a \equiv a \bmod n$.

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

From $a \equiv b \bmod n$, we obtain $n \mid a - b$. As we know, divisibilities do not care about signs, so this yields $n \mid -(a - b)$. But this means $n \mid b - a$. In other words, $b \equiv a \bmod n$.

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

From $a \equiv b \bmod n$, we see that $n \mid a - b$. Similarly, $n \mid b - c$. Hence, both $a - b$ and $b - c$ are multiples of n. Their sum $(a - b) + (b - c)$ must therefore be a multiple of n. But this sum is $a - c$. So we know that $n \mid a - c$. In other words, $a \equiv c \bmod n$.

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

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

We must prove that

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

From $a_1 \equiv b_1 \bmod n$, we obtain $n \mid a_1 - b_1$. In other words, $a_1 - b_1 = nc_1$ for some integer c_1.

Similarly, $a_2 - b_2 = nc_2$ for some integer c_2.

Consider these c_1 and c_2. From $a_1 - b_1 = nc_1$, we get $a_1 = b_1 + nc_1$. Similarly, $a_2 = b_2 + nc_2$.

Hence,

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

showing that $(a_1 + a_2) - (b_1 + b_2) = n(c_1 + c_2)$ is a multiple of n, and thus $a_1 + a_2 \equiv b_1 + b_2 \bmod n$.

Similarly,

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

showing that $(a_1 - a_2) - (b_1 - b_2) = n(c_1 - c_2)$ is a multiple of n, and thus $a_1 - a_2 \equiv b_1 - b_2 \bmod n$.

Finally,

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

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

So we have proved part **(d)**.

(e) Let $a, b \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$. Thus, $n \mid a - b$. Hence, $m \mid n \mid a - b$, so that $m \mid a - b$ (by the transitivity of divisibility). In other words, $a \equiv b \bmod m$. □

Part **(b)** of the above proposition shows that congruences can be turned around (unlike divisibilities).

Part **(c)** shows that congruences can be chained together. Such chains of congruences look like chains of divisibilities: The statement

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

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

Remark 3.2.5. Don't get overly enthusiastic about part **(d)**. It allows you to add, subtract and multiply congruences modulo n, but it does not allow you to divide them or to take one to the other's power. So

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

do not imply $a_1 / a_2 \equiv b_1 / b_2 \bmod n$ or $a_1^{a_2} \equiv b_1^{b_2} \bmod n$ (even if all of these numbers are integers).

Also note that congruences modulo different n's cannot be combined. For example, $a_1 \equiv b_1 \bmod 2$ and $a_2 \equiv b_2 \bmod 3$, then nothing follows about $a_1 a_2$ and $b_1 b_2$.

However, congruences can be taken to the k-th power for a fixed $k \in \mathbb{N}$:

Exercise 3.2.1. Let $n, a, b \in \mathbb{Z}$ such that $a \equiv b \bmod n$. Prove that $a^k \equiv b^k \bmod n$ for any $k \in \mathbb{N}$.

3.2.3. Proving the divisibility criteria

Now let us prove part **(e)** of our theorem about divisibility criteria, restating it as follows:

Proposition 3.2.6. Let $m \in \mathbb{N}$. Let s be the sum of the digits of m written in decimal. (For instance, if $m = 308$, then $s = 3 + 0 + 8 = 11$.)

Then, $9 \mid m$ if and only if $9 \mid s$.

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

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

However, $10 \equiv 1 \bmod 9$ (since $10 - 1 = 9$ is a multiple of 9). Hence, by the preceding exercise, we get

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

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

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

In other words,

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

Now, adding these congruences together for all $k \in \{0, 1, \ldots, d\}$, we obtain

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

In other words,

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

Turning this congruence around, we get $s \equiv m \bmod 9$.

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

Conversely, if $9 \mid s$, then $s \equiv 0 \bmod 9$, hence $m \equiv s \equiv 0 \bmod 9$, so that $m \equiv 0 \bmod 9$, and thus $9 \mid m$.

Altogether, this shows that $9 \mid m$ if and only if $9 \mid s$. □

The analogue of this proposition for 3 instead of 9 (i.e., part **(d)** of the above divisibility criteria theorem) is proved similarly, now using $10 \equiv 1 \bmod 3$ (which follows from $10 \equiv 1 \bmod 9$).

See Exercise 3.2.3 in the notes for a divisibility-by-11 criterion.

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. Consider the pair (q, r) whose existence and uniqueness is claimed by the theorem we just stated. Then:

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

For now, we do not yet know that (q, r) exists and is unique, so we will be using indefinite articles ("a quotient", "a remainder", "a quo-rem pair") until we have proved this.

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

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

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

Example 3.3.4. What are $23//5$ and $23\%5$? We have $23//5 = 4$ and $23\%5 = 3$.

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

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

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

So our theorem is saying that for any integer n and any positive integer d, there is a unique quo-rem pair of n and d. Let us now prove this.

3.3.2. 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.

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.

We shall prove this by contradiction. So we assume that (q_1, r_1) and (q_2, r_2) are two distinct quo-rem pairs of n and d. How do we get a contradiction?

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

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

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

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

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

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

Hence,

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

Now, 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, $q_2 - q_1 \geq 1$. Thus, $(q_2 - q_1)\, d \geq 1d = d$. Thus, we get

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

which contradicts

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

So we found a contradiction in Case 1.

Consider Case 2. In this case, $q_1 = q_2$. Now,

$$r_1 - r_2 = (q_2 - q_1)\, d = 0 \qquad (\text{since } q_1 = q_2),$$

so $r_1 = r_2$. Combining this with $q_1 = q_2$, we obtain $(q_1, r_1) = (q_2, r_2)$. So our two quo-rem pairs (q_1, r_1) and (q_2, r_2) are identical, which contradicts our assumption that they are distinct. Again a contradiction.

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

So we found a contradiction in each case. Thus, we always have a contradiction, and the proof of uniqueness is complete.

Now, let us come to the existence part. We want to prove it by strong induction on n, but there is a difficulty: We don't know where to start; n is just supposed to be an integer, not a nonnegative integer. But this is not unsurmountable! We can first prove the claim for $n \geq 0$, and then extend it to negative n's.

So let us first prove the $n \geq 0$ case (i.e., the $n \in \mathbb{N}$ 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 apply strong induction on n (without a base case):

Induction step: Let $n \in \mathbb{N}$. Assume (as the IH) that the lemma is proved 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 can be explicitly constructed: it is $(0, n)$ (since $n < d$ enntails $n \in \{0, 1, \ldots, d-1\}$).

Otherwise, $n \geq d$, so that $n - d \in \mathbb{N}$. Hence, we can apply the IH to $n - d$ instead of n (since $n - d < n$). This yields that there exists a quo-rem pair (q, r) of $n - d$ and d. Consider this pair. Now I claim that $(q+1, r)$ is a quo-rem pair of n and d. This is because

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

This shows that n and d have a quo-rem pair. This completes our induction step, and thus the lemma is proved. □

It remains to show that the quo-rem pair of n and d also exists when n is negative. One way to do this is by strong induction on $-n$ (since $-n$ will be positive).

Another way is by deducing the negative case from the positive case. Here is how this goes: Let n be a negative integer. Then, the product $\underbrace{(1-d)}_{\leq 0} \underbrace{n}_{<0}$ is nonnegative, so we can apply the lemma to this product $(1-d)\, n$ instead of n. We obtain a quo-rem pair (q, r) of $(1-d)\, n$ and d. This quo-rem pair satisfies

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

This shows that $(n+q, r)$ is a quo-rem pair of n and d.

The proof of the theorem is finally complete. □

3.3.3. An application: even and odd integers

Recall that an integer n is **even** if $2 \mid n$ and is **odd** if $2 \nmid n$. Now we claim the following:

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)** is a consequence of the definitions of "even" and "divisible".
(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 preceding theorem, there exists a quo-rem pair (q, r) of n and 2. Consider this pair. It satisfies $q \in \mathbb{Z}$ and $r \in \{0, 1\}$ and $n = 2q + r$. If r were 0, then this would imply $n = 2q + \underbrace{r}_{=0} = 2q$, which would make n even, not odd. But n is odd. So r cannot be 0. Hence, $r = 1$ (since $r \in \{0, 1\}$). Thus, $n = 2q + \underbrace{r}_{=1} = 2q + 1$. So there exists some $k \in \mathbb{Z}$ such that $n = 2k + 1$ (namely, $k = q$). This proves the $\Longrightarrow$ direction.

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 $2 \nmid n$. In other words, we must prove that n cannot be written as $2c$ for any $c \in \mathbb{Z}$.

Assume the contrary. So $n = 2c$ for some $c \in \mathbb{Z}$. Consider this c. Now, we have $n = 2k + 1$ but also $n = 2c = 2c + 0$. This means that both pairs $(k, 1)$ and $(c, 0)$ are quo-rem pairs of n and 2. But our theorem says that the quo-rem pair of n and 2 is unique. Hence, $(k, 1) = (c, 0)$. This is absurd, since $1 \neq 0$. This contradiction completes our proof. □

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

Proof. **(c)** By the previous proposition, any two odd integers can be written as $2k + 1$ and $2\ell + 1$ for some $k, \ell \in \mathbb{Z}$. Thus their sum is $(2k + 1) + (2\ell + 1) = 2k + 2\ell + 2 = 2(k + \ell + 1)$, which is even.
(a), **(b)** are similar. □

Remark 3.3.9. Part **(c)** of this corollary is specific to the number 2. It is not true that the sum of any two integers not divisible by 3 is divisible by 3.

3.3.4. Basic properties of quotients and remainders

Proposition 3.3.10. 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 $n//d \in \mathbb{N}$.

Parts **(a)** and **(c)** of this proposition show that the remainder $n\%d$ is characterized as the unique element of $\{0, 1, \ldots, d-1\}$ that is congruent to n modulo d.

Proof. We set

$$q := n//d \qquad \text{and} \qquad r := n\%d.$$

Then, (q, r) is a quo-rem pair of n and d. In other words,

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

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

(a) We have $n\%d = r \in \{0, 1, \ldots, d-1\}$. Moreover, $n\%d \equiv n \bmod d$ since

$$\underbrace{n\%d}_{=r} - \underbrace{n}_{=qd+r} = r - (qd + r) = -qd \text{ is a multiple of } d.$$

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

Since $c \equiv n \bmod d$, we have $d \mid c - n$. In other words, $c - n = ds$ for some integer s. Using this s, we have

$$n = c - ds = (-s)\, d + c.$$

This shows that $(-s, c)$ is a quo-rem pair of n and d. But (q, r) is also a quo-rem pair of n and d. Since the quo-rem pair of n and d is unique, this entails that $(-s, c) = (q, r)$. In particular, $c = r = n\%d$, qed.

(b) This is an "if and only if" statement. Let us prove its two directions separately:

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

From $d \mid n$, we obtain $n \equiv 0 \bmod d$, so that $0 \equiv n \bmod d$. Also, $0 \in \{0, 1, \ldots, d-1\}$. Hence, part **(c)** (applied to $c = 0$) yields $0 = n\%d$, so that $n\%d = 0$.

$\Longleftarrow$: 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) This can be proved by strong induction on n (just as we proved the lemma above) or by some inequality chasing (show that $q > -1$, and conclude that $q \geq 0$ because q is an integer). See the notes (Proposition 3.3.11 **(e)**) for details. □

Corollary 3.3.11. Let $n \in \mathbb{Z}$. Then:
(a) The integer n is even if and only if $n\%2 = 0$.
(b) The integer n is odd if and only if $n\%2 = 1$.

Proof. Easy using the above (see notes). □

Quotients and remainders are closely related to the so-called floor function:

Definition 3.3.12. The **integer part** (aka **floor**) of a real number x is defined to be the largest integer that is $\leq x$. It is denoted by $\lfloor x \rfloor$.

For example, $\lfloor 3.8 \rfloor = 3$ and $\lfloor \pi \rfloor = 3$ and $\lfloor 5 \rfloor = 5$ and $\lfloor -\pi \rfloor = -4$.

Proposition 3.3.13 ("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. See the notes. (Again, some basic inequality chasing.)
Main idea: To prove that $u = \lfloor x \rfloor$, it is sufficient (and necessary) to show that u is an integer and that $u \leq x < u + 1$. □

3.3.5. Base-b representation of nonnegative integers

Division with remainder is the main ingredient in positional number systems – i.e., base-b notation for integers.

What does this mean? For example,

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

Thus, the fairly large number 3401 has been written using just four digits.

This can be done for any nonnegative integer, but it can also be done with the 10 replaced by any number $b > 1$. In other words, any $n \in \mathbb{N}$ can be written as a sum of powers of b, where the coefficient in front of each power is a number between 0 and $b - 1$.

For example, let us do this for $n = 3401$ and $b = 4$. So we want to represent 3401 in 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 $\{0, 1, 2, 3\}$).

How do we find these digits r_i ? Let's start with r_0. We want

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

Since $r_0 \in \{0, 1, 2, 3\}$, this equality entails that

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

So we have found r_0. Perform the same operation with the equation

$$r_6 4^5 + r_5 4^4 + r_4 4^3 + r_3 4^2 + r_2 4^1 + r_1 4^0 = 850$$

to find

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

So we have found r_1. Perform the same operation with the equation

$$r_6 4^4 + r_5 4^3 + r_4 4^2 + r_3 4^1 + r_2 4^0 = 212$$

to find

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

So we have found r_2. Continuing along the same lines, we obtain $r_3 = 1$ and $r_4 = 1$ and $r_5 = 3$ and $r_6 = 0$. Thus,

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

In analogy to the decimal (i.e., base-10) representation, we can state this as "the number 3401 written in base-4 is 0311021". One usually omits leading zeroes, so this simplifies to 311021.

The method we just used can be applied to any given integer $b > 1$ instead of 4, and to any $n \in \mathbb{N}$ instead of 3401: To find the "base-b digits" of n, we first divide n by b with remainder, then divide the resulting quotient again by b with remainder, then divide the resulting quotient again by b with remainder, and so on. The remainders obtained will be the base-b digits of n (from right to left). Here is this method stated as a theorem:

Theorem 3.3.14. 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

There is a close connection between remainders and congruence:

Proposition 3.3.15. 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 know that $a\%d \in \{0, 1, \ldots, d-1\}$ and $a\%d \equiv a \bmod d$.

Now, we must prove the equivalence

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

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

$\Longrightarrow$: Assume that $a \equiv b \bmod d$. Then, $a\%d \equiv a \equiv b \bmod d$. So $a\%d$ is a number in $\{0, 1, \ldots, d-1\}$ that is congruent to b modulo d. But the only such number is $b\%d$. Consequently, $a\%d = b\%d$. This proves the $\Longrightarrow$ direction.

$\Longleftarrow$: Assume that $a\%d = b\%d$. We have shown that $a\%d \equiv a \bmod d$. Similarly, $b\%d \equiv b \bmod d$. Combining these, we find

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

So $a \equiv b \bmod d$. This proves the $\Longleftarrow$ direction. □

Corollary 3.3.16. Let a and b be two integers. Then, $a \equiv b \bmod 2$ if and only if the numbers a and b are both even or both odd.

3.3.7. The birthday lemma

If you have lived for exactly n days, then you are $n//365$ years and $n\%365$ days old, assuming that there are no leapyears. On any regular day, the number $n//365$ remains unchanged, whereas the number $n\%365$ increases by 1. On a birthday, $n//365$ increases by 1, whereas the number $n\%365$ is reset to 0. Let us state this in full generality:

Proposition 3.3.17 (birthday lemma)**.** Let $n \in \mathbb{Z}$, and let d be a positive integer. Then:

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

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

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

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

Proof. Easy; see the notes. □

Note that the quotient equalities in the above proposition can be rewritten as

$$\underbrace{\left\lfloor \frac{n}{d} \right\rfloor = \left\lfloor \frac{n-1}{d} \right\rfloor + 1}_{\text{when } d \mid n}, \qquad \text{resp.} \qquad \underbrace{\left\lfloor \frac{n}{d} \right\rfloor = \left\lfloor \frac{n-1}{d} \right\rfloor}_{\text{when } d \nmid n}.$$

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 refer to it as the **gcd** of a and b.

Examples:

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

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

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

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

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

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

  The divisors of 0 are all the integers.

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

  So the common divisors of 0 and 5 are just the divisors of 5, and the greatest of them is 5.

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

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

  By definition, $\gcd(0,0)=0$, although every integer is a common divisor of 0 and 0.

This method for computing gcds is not a good one when the numbers become large. We will soon see a better one. But first, we need to learn a few things about gcds. Let us start with the very basics. First, we observe that $\gcd(a,b)$ is always well-defined, because

- if $a=b=0$, then it is defined to be 0;
- if $a\neq 0$, then every divisor of a is $\leq |a|$, so that a has only finitely many divisors;
- if $b\neq 0$, then every divisor of b is $\leq |b|$, so that b has only finitely many divisors;
- in either case, a and b have at least one common divisor (namely, 1), so we are not taking the maximum of an empty set.

(Details in the notes.)

3.4.2. Basic properties

Proposition 3.4.2. We have $\gcd(a,b)\in\mathbb{N}$ for any $a,b\in\mathbb{Z}$.

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

In the remaining case, $\gcd(a,b)$ is literally the largest common divisor of a and b. But if it was negative, then $-\gcd(a,b)$ would be a 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 3.4.3. We have $\gcd(a,0) = \gcd(0,a) = |a|$ for every $a \in \mathbb{Z}$.

Proof. Every integer is a divisor of 0. So the common divisors of a and 0 are just the divisors of a. But the largest divisor of a is $|a|$ (unless $a = 0$, which case is trivial anyway). So we are done. □

Proposition 3.4.4. We have $\gcd(a,b) = \gcd(b,a)$ for every $a, b \in \mathbb{Z}$.

Proof. To be a common divisor of a and b is the same as being a common divisor of b and a. □

Proposition 3.4.5. Let $a, b, c \in \mathbb{Z}$ satisfy $b \equiv c \bmod a$. Then, $\gcd(a,b) = \gcd(a,c)$.

Proof. If $a = 0$, then $b \equiv c \bmod a$ entails $b = c$, so this is obvious.

Now let us consider the case $a \neq 0$. In this case, the gcds are literal largest common divisors. We will show that the common divisors of a and b are precisely the common divisors of a and c. To do so, 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 prove that d is a common divisor of a and c. It suffices to show that $d \mid c$ (since $d \mid a$ follows from the definition of d).

Recall that $b \equiv c \bmod a$, so that $c \equiv b \bmod a$. In other words, $a \mid c - b$. Hence, $d \mid a \mid c - b$. But also $d \mid b$. Therefore, $d \mid (c - b) + b$ (since the sum of two multiples of d is again a multiple of d). In other words, $d \mid c$. This proves Claim 1. □

Proof of Claim 2. This is just Claim 1 with the roles of b and c interchanged. (Keep in mind that $b \equiv c \bmod a$ implies $c \equiv b \bmod a$, so that b and c play equal roles.) □

Having proved Claim 1 and Claim 2, we see that the common divisors of a and b are precisely the common divisors of a and c. Thus, $\gcd(a,b) = \gcd(a,c)$. □

Proposition 3.4.6. For any $a, b, u \in \mathbb{Z}$, we have $\gcd(a,b) = \gcd(a,\ ua + b)$.

Proof. Follows from the previous proposition, since $b \equiv ua + b \bmod a$. □

Proposition 3.4.7. We have $\gcd(a,b) = \gcd(a,\ b\%a)$ for any positive integer a and any $b \in \mathbb{Z}$.

Proof. Follows from two propositions ago (applied to $c = b\%a$), since $b\%a \equiv b \bmod a$. □

Three more very easy facts:

Proposition 3.4.8. We have $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$ for any $a, b \in \mathbb{Z}$.

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

Proposition 3.4.10. If $a, b \in \mathbb{Z}$ satisfy $a \mid b$, then $\gcd(a,b) = |a|$.

Corollary 3.4.11 (Euclidean recursion for the gcd)**.** Let $a \in \mathbb{Z}$. 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 one of the propositions above, applied to b and a instead of a and b). □

3.4.3. The Euclidean algorithm

By applying this corollary repeatedly, we can find gcds very quickly. For instance,

$$\begin{aligned}
\gcd(30,\ 82) &= \gcd(82,\ 30\%82) && \text{(by the corollary)} \\
&= \gcd(82,\ 30) \\
&= \gcd(30,\ 82\%30) && \text{(by the corollary)} \\
&= \gcd(30,\ 22) \\
&= \gcd(22,\ 30\%22) && \text{(by the corollary)} \\
&= \gcd(22,\ 8) \\
&= \gcd(8,\ 22\%8) && \text{(by the corollary)} \\
&= \gcd(8,\ 6) \\
&= \gcd(6,\ 8\%6) && \text{(by the corollary)} \\
&= \gcd(6,\ 2) \\
&= \gcd(2,\ 6\%2) && \text{(by the corollary)} \\
&= \gcd(2,\ 0) \\
&= |2| && \text{(by the proposition } \gcd(a,0) = |a|) \\
&= 2
\end{aligned}$$

and

$$\begin{aligned}
&\gcd(745,\ 239)\\
&= \gcd(239,\ 745\%239) \qquad \text{(by the corollary)}\\
&= \gcd(239,\ 28)\\
&= \gcd(28,\ 239\%28) \qquad \text{(by the corollary)}\\
&= \gcd(28,\ 15)\\
&= \gcd(15,\ 28\%15) \qquad \text{(by the corollary)}\\
&= \gcd(15,\ 13)\\
&= \gcd(13,\ 15\%13) \qquad \text{(by the corollary)}\\
&= \gcd(13,\ 2)\\
&= \gcd(2,\ 13\%2) \qquad \text{(by the corollary)}\\
&= \gcd(2, 1)\\
&= \gcd(1, 2\%1) \qquad \text{(by the corollary)}\\
&= \gcd(1, 0)\\
&= |1| = 1.
\end{aligned}$$

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, this looks as follows:

```
def gcd(a, b):  # for b nonnegative
    if b == 0:
        return abs(a) # this is |a| in Python
    return gcd(b, a%b)
```

This algorithm is known as the **Euclidean algorithm**. Let us convince ourselves that it really terminates (i.e., does not get stuck in an infinite loop):

Proposition 3.4.12. Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then, the Euclidean algorithm terminates after at most b steps.

Proof. In every step, we replace b by $a\%b$. This decreases b by at least 1 (since $a\%b \leq b - 1$). If we make b such decreases, b will thus become 0 or smaller. But at that point, the algorithm must stop. So the algorithm cannot survive for more than b steps. □

This is, of course, an overestimate of how long the algorithm will take. A better bound for the running time is $\log_2(ab) + 2$ (if a and b are positive). See the notes for why this is a bound. This shows that the Euclidean algorithm computes $\gcd(a,b)$ a lot faster than the naive "list all divisors of a and all divisors of b" approach would do.

We can easily adapt the Euclidean algorithm to work for all $b \in \mathbb{Z}$ (not just for $b \in \mathbb{N}$):

```
def gcd(a, b):
    if b < 0:
        return gcd(a, -b)
    if b == 0:
        return abs(a) # this is |a| in Python
    return gcd(b, a%b)
```

3.4.4. Bezout's theorem and the extended Euclidean algorithm

The Euclidean algorithm can be adapted so that it computes not only $\gcd(a,b)$, but also a way to express $\gcd(a,b)$ as an "integer linear combination" of a and b (that is, as a multiple of a plus a multiple of b). This allows us to prove the following theorme:

Theorem 3.4.13 (Bezout's theorem for integers)**.** Let a and b be two integers. Then, there exist two integers x and y such that

$$\gcd(a,b) = xa + yb.$$

We shall prove this in a moment. First, a notation:

Definition 3.4.14. Let a and b be two integers. Then, a **Bezout pair** for (a,b) means a pair (x,y) of two integers such that $\gcd(a,b) = xa + yb$.

So Bezout's theorem says that any pair (a,b) of integers has a Bezout pair. Examples:

- Can you find a Bezout pair for $(4,7)$? That would be a pair (x,y) of two integers such that $\underbrace{\gcd(4,7)}_{=1} = x \cdot 4 + y \cdot 7$. For example, $(2,-1)$ is such a pair, since $1 = 2 \cdot 4 + (-1) \cdot 7$. Note that this is a version of the coin problem we have discussed a while ago, but now we allow change.
- Can you find a Bezout pair for $(3,8)$? For instance, $(-5,2)$ works; so does $(3,-1)$.
- Can you find a Bezout pair for $(3,3)$? For instance, $(1,0)$ or $(0,1)$.

So Bezout's theorem says that $\gcd(a,b)$ cents can be paid using a-cent coins and b-cent coins if change is allowed. We will soon discuss the same problem without change.

How can we prove Bezout's theorem? First, we observe that if (x,y) is a Bezout pair for (a,b), then $(x,-y)$ is a Bezout pair for $(a,-b)$ (since $xa+(-y)(-b) = xa+yb$ and $\gcd(a,-b) = \gcd(a,b)$). Thus, in proving the theorem, we only need to deal with the case $b \geq 0$. In other words, it suffices to prove the following lemma:

Lemma 3.4.15. Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then, there exists a Bezout pair for (a,b).

Proof. We strongly induct on b. We do not consider a as being fixed. Thus, the statement that we will be proving is

$$P(b) := (\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a,b)).$$

We must prove this statement $P(b)$ for all $b \in \mathbb{N}$. We shall do this by strong induction on b:

Base case: Let us prove the statement $P(0)$. This is saying that for each $a \in \mathbb{Z}$, there exists a Bezout pair for $(a,0)$, that is, a pair (x,y) of two integers such that $\underbrace{\gcd(a,0)}_{=|a|=\pm a} = xa+y0$. This is easy: $(x,y) = (\pm 1, 0)$. So the base case is done.

Induction step: Let b be a positive integer. We must prove the implication

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

So we assume (as the IH) that $P(0)$ AND $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(b-1)$ holds. In other words, we assume that

$$\begin{aligned}&(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a,0)) \text{ and}\\ &(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a,1)) \text{ and}\\ &(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a,2)) \text{ and}\\ &\cdots \text{ and}\\ &(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a,b-1)).\end{aligned}$$

In yet other words, we assume that for each $a \in \mathbb{Z}$ and each $d \in \{0,1,\ldots,b-1\}$, there exists a Bezout pair for (a,d).

Our goal is now to prove $P(b)$. In other words, we must prove that for each $a \in \mathbb{Z}$, there exists a Bezout pair for (a,b).

So we fix $a \in \mathbb{Z}$, and we set out to find a Bezout pair for (a,b).

The Euclidean recursion yields

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

Since $a\%b \in \{0, 1, \ldots, b-1\}$, this allows us to apply the IH to b and $a\%b$ instead of a and d. So we conclude that there exists a Bezout pair (u, v) for $(b,\ a\%b)$. Consider this pair. Thus, u and v are integers and

$$\gcd(b,\ a\%b) = ub + v(a\%b).$$

Thus,

$$\begin{aligned}\gcd(a,b) = \gcd(b,\ a\%b) &= ub + v \underbrace{(a\%b)}_{\substack{=a-(a//b)b \\ (\text{since } a=(a//b)b+(a\%b))}} \\ &= ub + v(a - (a//b)\, b) \\ &= va + (u - v(a//b))\, b.\end{aligned}$$

This shows that $(v,\ u - v(a//b))$ is a Bezout pair for (a, b). So such a Bezout pair does exist. This concludes the proof of $P(b)$. So the induction step is complete, and the lemma is proved. □

As we said, the lemma entails the theorem.

The above inductive proof contains a recursive algorithm for finding a Bezout pair for (a, b) whenever $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. This is known as the **extended Euclidean algorithm**, and has the following form in Python:

```
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))
where
def sign(a):
    if a < 0:  return -1
    if a == 0:  return 0
    if a > 0:  return 1
```

To extend the above code to negative b, just add an extra "if $b < 0$" check which flips the signs of b and of v.

3.4.5. The universal property of the gcd

Bezout's theorem can be used to obtain the following important property of gcds:

Theorem 3.4.16 (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 $\gcd(a,b)$.

Proof of the universal property. The $\Longleftarrow$ direction is easy: If $m \mid \gcd(a,b)$, then $m \mid a$ (since $m \mid \gcd(a,b) \mid a$) and $m \mid b$ (similarly).

Now for the $\Longrightarrow$ direction: Assume that $m \mid a$ and $m \mid b$. We must prove that $m \mid \gcd(a,b)$.

Bezout's theorem says that $\gcd(a,b)$ can be written as $\gcd(a,b) = xa + yb$ for some integers x and y. Consider these x and y.

Now, xa is a multiple of m (since $m \mid a \mid xa$), and so is yb (since $m \mid b \mid yb$). Hence, their sum $xa + yb$ is also a multiple of m. But this sum is $\gcd(a,b)$. Thus, we see that $\gcd(a,b)$ is a multiple of m. In other words, $m \mid \gcd(a,b)$. □

This universal property can in turn be used to prove many other properties of gcds, for example:

Exercise 3.4.1. Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ be integers satisfying $a_1 \mid b_1$ and $a_2 \mid b_2$. Prove that $\gcd(a_1, a_2) \mid \gcd(b_1, b_2)$.

3.4.6. Factoring out a common factor from a gcd

The following theorem "feels" obvious, but is not:

Theorem 3.4.17. 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 $h = |s| \cdot g$. Since h and g are nonnegative, this is equivalent to proving that $|h| = |sg|$ (since $|h| = h$ and $|g| = g$ and $|sg| = |s| \cdot |g| = |s| \cdot g$). In order to do this, it suffices to show that $h \mid sg$ and $sg \mid h$ (because we proved a fact a while ago that $x \mid y$ and $y \mid x$, then $|x| = |y|$).

So let us show this.

- *Proof of $sg \mid h$:* We must prove $sg \mid h$. In other words, we must prove $sg \mid \gcd(sa, sb)$. By the universal property of the gcd, this is equivalent to proving that $sg \mid sa$ and $sg \mid sb$. But $sg \mid sa$ follows from $g \mid a$, whereas $sg \mid sb$ follows from $g \mid b$. So we are done with the proof of $sg \mid h$.

- *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.

  Bezout's theorem shows that $g = \gcd(a,b) = xa + yb$ for some integers x and y. Consider these x and y.

Now,

$$\begin{aligned} sg &= s\left(xa+yb\right) = sxa+syb = x\underbrace{sa}_{=hu}+y\underbrace{sb}_{=hv} \\ &= xhu+yhv = h\left(xu+yv\right), \end{aligned}$$

which shows that $h \mid sg$.

(The notes also give an other proof – see the proof of Theorem 3.4.11.)

□

3.5. Coprime integers

3.5.1. Definition and examples

Greatest common divisors are at their most useful when they equal 1. This is called "coprimality":

Definition 3.5.1. Two integers a and b are said to be **coprime** (or **relatively prime**) if $\gcd\left(a,b\right) = 1$.

Remark 3.5.2. This is a symmetric relation: If a and b are coprime, then b and a are coprime (since $\gcd\left(a,b\right) = \gcd\left(b,a\right)$).

Example 3.5.3. (a) An integer n is coprime to 2 if and only if n is odd. Indeed, $\gcd\left(n,2\right)$ is a nonnegative divisor of 2, so it is always either 1 or 2. If n is even, then it is 2 (since $2 \mid n$ and $2 \mid 2$ in this case). If n is odd, then it is 1 (since $2 \nmid n$ shows that it cannot be 2).

(b) An integer n is coprime to 3 if and only if n is not divisible by 3 (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 only nonnegative divisors of 4 are 1, 2 and 4, so that $\gcd\left(n,4\right)$ is always 1, 2 or 4. If n is even, then it is 2 or 4, since 2 is a common divisor of n and 4. If n is odd, then it has to be 1, since neither 2 nor 4 divides n.)

(d) An integer n is coprime to 5 if and only if n is not divisible by 5 (since the only nonnegative divisors of 5 are 1 and 5).

(e) An integer n is coprime to 6 if and only if n is neither even nor divisible by 3.

(Indeed, $\gcd\left(n,6\right)$ is 1, 2, 3 or 6. If n is even, then it is ≥ 2, since 2 is a common divisor of n and 6. If n is divisible by 3, then it is ≥ 3 for a similar reason. If n is neither, then 2, 3 and 6 are out of the question, and therefore $\gcd\left(n,6\right) = 1$.)

Informally, I think of coprimality as a sort of "unrelatedness" or "independence" or "orthogonality" relation between numbers, as far as their divisors are concerned.

3.5.2. Three theorems about coprimality

The following three theorems make coprimality useful:

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 $ba \mid bc$ (because $a \mid c$). In other words, $ab \mid ca$ and $ab \mid cb$. So $ab \mid \gcd(ca, cb)$ by the universal property of the gcd. Thus,

$$ab \mid \gcd(ca, cb) = |c| \cdot \underbrace{\gcd(a, b)}_{\substack{=1 \\ \text{(since } a \text{ and } b \\ \text{are coprime)}}} \qquad \text{(by the previous theorem)}$$
$$= |c| .$$

Since divisibility does not depend on 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, this entails $4 \cdot 7 \mid 56$.

In contrast, $6 \mid 12$ and $4 \mid 12$ do not entail $6 \cdot 4 \mid 12$, 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

$$a \mid \gcd(ca, cb) = |c| \cdot \underbrace{\gcd(a, b)}_{\substack{=1 \\ \text{(since } a \text{ and } b \\ \text{are coprime)}}} = |c| ,$$

so that $a \mid c$. □

Example 3.5.7. From $6 \mid 7 \cdot 12$, we conclude that $6 \mid 12$, since 6 is coprime to 7.

However, from $6 \mid 12 \cdot 7$, we cannot conclude that $6 \mid 7$, since 6 is not coprime to 12.

Theorem 3.5.8 (coprime product theorem)**.** Let $a, b, c \in \mathbb{Z}$ be such that each of the numbers 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 $g = \gcd(ab, c) \mid c \mid ac$. Thus, the universal property of the gcd yields

$$g \mid \gcd(ab, ac) = |a| \cdot \underbrace{\gcd(b, c)}_{=1} = |a|.$$

Thus, $g \mid a$. Combining this with $g \mid c$, we obtain $g \mid \gcd(a, c)$ (by the universal property again). In other words, $g \mid 1$ (since $\gcd(a, c) = 1$). Since g is a nonnegative integer, this entails that $g = 1$, and we are done. □

(See the notes for more general versions of these three theorems.)

3.5.3. Reducing a fraction

Theorem 3.5.9. 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 ratio $\frac{u}{v}$ of two integers is said to be in **reduced form** if u and v are coprime. So the theorem is saying that if we start with a ratio $\frac{a}{b}$ of two integers, and cancel $\gcd(a, b)$ from its numerator and its denominator, then we get a ratio in reduced form. Hence, any rational number can be brought to a reduced form.

Proof of the theorem. Easily, $g > 0$ (since it is the gcd of the integers a and b, which are not both 0). Hence, $|g| = g$.

The numbers $\frac{a}{g}$ and $\frac{b}{g}$ are integers since $g = \gcd(a, b) \mid a$ and $g = \gcd(a, b) \mid b$. Moreover,

$$\begin{aligned} g = \gcd(a, b) &= \gcd\left(g\frac{a}{g}, g\frac{b}{g}\right) = |g| \cdot \gcd\left(\frac{a}{g}, \frac{b}{g}\right) \\ &= g \cdot \gcd\left(\frac{a}{g}, \frac{b}{g}\right). \end{aligned}$$

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. □

3.6. Prime numbers

3.6.1. Definition

Here comes one of the most famous concepts in mathematics:

Definition 3.6.1. An integer $n > 1$ is said to be **prime** (or **a prime**) if the only positive divisors of n are 1 and n.

The first few primes (= prime numbers) are

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43.$$

It can be shown that there are infinitely many primes (see the HW).

3.6.2. The friend-or-foe lemma

The first property of primes we will prove is the **friend-or-foe lemma**:

Lemma 3.6.2 (friend-or-foe lemma)**.** Let p be a prime. Let $n \in \mathbb{Z}$. Then, n is either divisible by p or coprime to p, but not both.

Proof. The only positive divisors of p are 1 and p (since p is prime). Thus, $\gcd(n,p)$ must be either 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. This also shows that n is not divisible by p (because if it was, then p would be a common divisor of n and p, so that $\gcd(n,p)$ would be $\geq p$, contradicting $\gcd(n,p) = 1$). Hence, the lemma is proved in Case 1.

Now consider Case 2. In this case, we have $\gcd(n,p) = p > 1$, 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, too. □

In contrast, for a non-prime number $p > 1$, there exist integers n that are neither coprime to nor divisible by p. For instance, 2 is neither coprime to nor divisible by 6.

3.6.3. Binomial coefficients and primes

One of many applications of the friend-or-foe lemma is a property of binomial coefficients. Looking at Pascal's triangle, we might observe that all entries in the p-th row (i.e., all binomial coefficients $\binom{p}{k}$) except for the two 1's at the ends are divisible by p when p is a prime. This is indeed the case:

Theorem 3.6.3. Let p be a prime. Let $k \in \{1,2,\ldots,p-1\}$. Then, $p \mid \binom{p}{k}$.

Proof. Exercise 5 **(a)** on HW#3 says that

$$k\binom{p}{k} = p\underbrace{\binom{p-1}{k-1}}_{\text{an integer}}.$$

This shows that $p \mid k\binom{p}{k}$. If we can show that p is coprime to k, then this will yield $p \mid \binom{p}{k}$ (by the coprime removal theorem), and we will be done.

So let us 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 (because $k \in \{1, 2, \ldots, p-1\}$), we conclude that k is coprime to p. That is, p is coprime to k, exactly as desired. □

3.6.4. Fermat's little theorem

It is easy to see that every integer a satisfies $a^2 \equiv a \bmod 2$. (Indeed, this is saying that $2 \mid a^2 - a = a(a-1)$, which is true since one of a and $a-1$ will always be even.)

Likewise, every integer a satisfies $a^3 \equiv a \bmod 3$ (since $a^3 - a = a\left(a^2-1\right) = (a+1)\,a\,(a-1)$ is divisible by 3).

This pattern breaks down for 4: Not every integer a satisfies $a^4 \equiv a \bmod 4$ (for example, 2 does not).

However, the pattern reappears for 5: Every integer a satisfies $a^5 \equiv a \bmod 5$. (But this does not follow that easily from factoring the difference: $a^5 - a = a(a-1)(a+1)\left(a^2+1\right)$. Nevertheless, there is a fully mechanical proof of this congruence, just using the remainder $a\%5$.)

The pattern breaks down again for 6, but reemerges for 7.

It seems that the pattern works for all primes. And it does:

Theorem 3.6.4 (Fermat's Little Theorem)**.** Let p be a prime. Let $a \in \mathbb{Z}$. Then,

$$a^p \equiv a \bmod p.$$

Proof. We induct on a. This will only cover the case $a \geq 0$, so we will have to use a separate argument for $a < 0$ afterwards.

Base case: The case $a^p \equiv a \bmod p$ clearly holds for $a = 0$ (since $0^p = 0$ and thus $0^p \equiv 0 \bmod p$).

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

$$\begin{aligned}
(a+1)^p &= \sum_{k=0}^{p} \binom{p}{k} a^k \underbrace{1^{p-k}}_{=1} = \sum_{k=0}^{p} \binom{p}{k} a^k \\
&= \underbrace{\binom{p}{0}}_{=1} \underbrace{a^0}_{=1} + \sum_{k=1}^{p-1} \binom{p}{k} a^k + \underbrace{\binom{p}{p}}_{=1} a^p \\
&= 1 + \underbrace{\sum_{k=1}^{p-1} \binom{p}{k} a^k}_{\substack{\text{This sum is divisible by } p, \\ \text{since our previous theorem} \\ \text{shows that } p \mid \binom{p}{k} \text{ for each } k \in \{1,2,\ldots,p-1\}}} + a^p \\
&\equiv 1 + \underbrace{a^p}_{\substack{\equiv a \bmod p \\ \text{(by the IH)}}} \equiv 1 + a = a + 1 \bmod p.
\end{aligned}$$

(See the notes for some more details on this argument.)

So the induction is complete, and the theorem is proved for all $a \geq 0$. It remains to prove it for all $a < 0$.

So let $a < 0$ be an integer. We must show that $a^p \equiv a \bmod p$.

Let $b := a\%p$. Then, $b \geq 0$, so that $b^p \equiv b \bmod p$ by the part of the theorem that we already have proved. But $b = a\%p \equiv a \bmod p$, so that $b^p \equiv a^p \bmod p$. Therefore,

$$a^p \equiv b^p \equiv b \equiv a \bmod p.$$

So the theorem holds for our a as well. This completes the proof. □

Curiosity: Fermat's Little Theorem does not have a converse! There are several non-prime numbers p such that every integer a satisfies $a^p \equiv a \bmod p$. For instance, 561 is such a p. The number $561 = 3 \cdot 11 \cdot 17$ is not prime, but every integer a satisfies $a^{561} \equiv a \bmod 561$. These are known as **Carmichael numbers**.

3.6.5. Prime divisor separation theorem

You can think of the primes as "inseparable" positive integers: They cannot be factored into two smaller positive integers.

But there is a deeper way in which this "inseparability" holds: If a prime p divides a product ab, then p must divide one of the factors. Let us state this as a theorem:

Theorem 3.6.5 (prime divisor separation theorem)**.** Let p be a prime. Let $a, b \in \mathbb{Z}$ be such that $p \mid ab$. Then, $p \mid a$ or $p \mid b$.

Proof. Let us prove this in the following equivalent form: "If $p \nmid a$, then $p \mid b$".

Assume that $p \nmid a$. We must prove that $p \mid b$.

The friend-or-foe lemma yields that a is either divisible by p or coprime to p. Since $p \nmid a$, this shows that a must be coprime to p. In other words, p is coprime to a. Thus, by the coprime removal theorem, from $p \mid ab$ we obtain $p \mid b$. Proof complete. □

Note that this theorem does not work for composite (= non-prime) numbers instead of p. For instance, $4 \mid 2 \cdot 6$ but $4 \nmid 2$ and $4 \nmid 6$.

We can extend the theorem to products of several factors:

Corollary 3.6.6 (prime divisor separation theorem for k factors)**.** Let p be a prime. Let $a_1, a_2, \ldots, a_k$ be integers 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 integers, then it divides at least one factor.)

Proof. Induct on k. The *base case* ($k = 0$) is vacuously true (since $p \nmid 1$). In the *induction step* from k to $k+1$, observe that $p \mid a_1 a_2 \cdots a_{k+1} = (a_1 a_2 \cdots a_k)\, a_{k+1}$, and use the theorem to conclude that $p \mid a_1 a_2 \cdots a_k$ or $p \mid a_{k+1}$, but in the first case we can use the induction hypothesis. □

3.6.6. p-valuations: definition

We will need the following simple lemma:

Lemma 3.6.7. 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. The relation $p^m \mid n$ means that $\dfrac{n}{p^m} \in \mathbb{Z}$. In other words, it means that we can divide n by p at least m times without getting a non-integer. So the lemma claims that there is a largest number of times that we can divide n by p without getting a non-integer. But this is true, because every time we divide n by p, the value $|n|$ decreases, which cannot keep happening forever without violating integrality.

(Alternatively, any $m \geq |n|$ will satisfy $p^m \geq p^{|n|} > |n|$, so that $p^m \nmid n$.) □

This lemma allows us to make the following definition:

Definition 3.6.8. Let p be a prime.

(a) Let n be a nonzero integer. Then, $v_p(n)$ shall denote the largest $m \in \mathbb{N}$ such that $p^m \mid n$. (We just showed that this largest m exists.) Thus, $v_p(n)$

is the largest number of times that you 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) In order for $v_p(n)$ to be defined for all n, we also define $v_p(0)$ to be ∞. This ∞ is a symbol, not an actual number, but we shall pretend that it behaves like a number in some regards. In particular, we can use it in addition and comparisons, following the rules

$$\begin{aligned}
k + \infty = \infty + k = \infty \qquad & \text{for all } k \in \mathbb{Z}; \\
\infty + \infty = \infty; & \\
k < \infty \qquad \text{and} \qquad \infty > k \qquad & \text{for all } k \in \mathbb{Z}; \\
\max\{\infty, k\} = \max\{k, \infty\} = \infty \qquad & \text{for all } k \in \mathbb{Z} \cup \{\infty\}; \\
\min\{\infty, k\} = \min\{k, \infty\} = k \qquad & \text{for all } k \in \mathbb{Z} \cup \{\infty\}.
\end{aligned}$$

Never subtract anything from ∞ (or ∞ from anything), because (e.g.) we have $1 + \infty = 0 + \infty$ but $1 \neq 0$.

Thus, ∞ acts like a "mythical number that is larger than any actual number". It acts its role well as long as we only take sums, minima and maxima.

Here are some examples:

$$\begin{aligned}
v_3(99) &= 2 \qquad \left(\text{since } 3^2 \mid 99 \text{ but } 3^3 \nmid 99\right); \\
v_3(98) &= 0 \qquad \left(\text{since } 3^0 \mid 98 \text{ but } 3^1 \nmid 98\right); \\
v_3(96) &= 1 \qquad \left(\text{since } 3^1 \mid 96 \text{ but } 3^2 \nmid 96\right); \\
v_3(0) &= \infty.
\end{aligned}$$

Here is another way to restate the definition of $v_p(n)$: 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, 344 is written 101011000 in base 2, so that $v_2(344) = 3$.

Our definition of $v_p(n)$ can be generalized to any positive integer $p > 1$ instead of a prime. But the more interesting properties of $v_p(n)$ rely on p being prime.

3.6.7. p-valuations: basic properties

Lemma 3.6.9. Let p be a prime. Let $i \in \mathbb{N}$ and $n \in \mathbb{Z}$. Then, $p^i \mid n$ if and only if $v_p(n) \geq i$.

Proof. If $n = 0$, then this is clear (since $p^i \mid 0 = n$ and $v_p(n) = v_p(0) = \infty \geq i$ in this case).

Let us now deal with the remaining case ($n \neq 0$). In this case, $v_p(n)$ is (by definition) the largest $m \in \mathbb{N}$ such that $p^m \mid n$. Hence, in this case, $p^i \mid p^{v_p(n)} \mid n$ whenever $i \leq v_p(n)$, whereas $p^i \nmid n$ whenever $i > v_p(n)$. Thus, $p^i \mid n$ if and only if $i \leq v_p(n)$. This proves the lemma. □

Theorem 3.6.10 (basic properties of p-valuations)**.** Let p be a prime. Then:
(a) We have $v_p(ab) = v_p(a) + v_p(b)$ for any $a, b \in \mathbb{Z}$.
(b) We have $v_p(a+b) \geq \min\{v_p(a),\ v_p(b)\}$ 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 is saying that $\infty = \infty + v_p(b)$, which is obvious. Similarly for $b = 0$. Thus, we only need to consider the case when a and b are both nonzero.

In this case, let

$$n = v_p(a) \qquad \text{and} \qquad m = v_p(b).$$

So $p^n \mid a$ but $p^{n+1} \nmid a$, and likewise $p^m \mid b$ but $p^{m+1} \nmid b$.

We want to prove that $v_p(ab) = n + m$. In other words, we want to prove that $p^{n+m} \mid ab$ but $p^{n+m+1} \nmid ab$.

From $p^n \mid a$, we get $a = p^n x$ for some integer x. This integer x cannot be divisible by p (since that would mean $x = px'$ for an integer x', so that $a = p^n x = p^n p x' = p^{n+1} x'$, contradicting $p^{n+1} \nmid a$).

So we have written $a = p^n x$ for some integer x that is not divisible by p.

Similarly, we write $b = p^m y$ for some integer y that is not divisible by p.

Thus, $ab = p^n x \cdot p^m y = p^{n+m} xy$. So $p^{n+m} \mid ab$.

Now why is $p^{n+m+1} \nmid ab$? Because if we had $p^{n+m+1} \mid ab$, then we would have $p^{n+m} p = p^{n+m+1} \mid ab = p^{n+m} xy$, so that (by cancelling p^{n+m}) we would find $p \mid xy$, which would yield (by the prime divisor separation theorem) that $p \mid x$ or $p \mid y$, contradicting the fact that neither x nor y is divisible by p.

So we have proved that $p^{n+m} \mid ab$ but $p^{n+m+1} \nmid ab$. Thus, $v_p(ab) = n + m = v_p(a) + v_p(b)$, qed.

(b) Let $a, b \in \mathbb{Z}$. We must prove that $v_p(a+b) \geq \min\{v_p(a),\ v_p(b)\}$.

If $a = 0$ or $b = 0$, this is easy. So we only care about the case when $a, b \neq 0$.

Let $k = \min\{v_p(a),\ v_p(b)\}$. Then, both a and b are multiples of p^k (why?). Hence, $a + b$ is a multiple of p^k. Hence, by the lemma above, $v_p(a+b) \geq k = \min\{v_p(a),\ v_p(b)\}$.

(c) This follows from $p^0 = 1 \mid 1$ but $p^1 = p \nmid 1$.

(d) This follows from $p^1 = p \mid p$ but $p^2 \nmid p$.

(e) Let $q \neq p$ be a prime. Then, the only positive divisors of q are 1 and q. In particular, p is not among them. So $p \nmid q$, that is, $p^1 \nmid q$. But $p^0 = 1 \mid q$. Thus, $v_p(q) = 0$. □

Corollary 3.6.11. Let p be a prime. Then,

$$v_p(a_1 a_2 \cdots a_k) = v_p(a_1) + v_p(a_2) + \cdots + v_p(a_k)$$

for any k integers $a_1, a_2, \ldots, a_k$.

Proof. Induct on k. The base case uses $v_p(1) = 0$. The step relies on part **(a)** of the theorem. □

3.6.8. Back to Hanoi

Proposition 3.6.12. Let $n \in \mathbb{N}$. Recall our strategy for solving the Tower of Hanoi puzzle with n disks.

Let $k \in \{1, 2, \ldots, 2^n - 1\}$. Then, the k-th move of our strategy moves the $(v_2(k) + 1)$-th smallest disk.

In particular, every odd move moves the smallest disk (since $v_2(k) = 0$ when k is odd).

For a proof, see the notes (§3.6.9).

The sequence

$$\begin{aligned}&(v_2(1),\ v_2(2),\ v_2(3),\ v_2(4),\ \ldots)\\ &= (0,\ 1,\ 0,\ 2,\ 0,\ 1,\ 0,\ 3,\ 0,\ 1,\ 0,\ 2,\ 0,\ 1,\ 0,\ 4,\ \ldots)\end{aligned}$$

is called the **ruler sequence**.

3.6.9. The p-valuation of $n!$

What is the p-valuation of a factorial $n!$? There is a nice formula:

Theorem 3.6.13 (de Polignac's formula)**.** Let p be a prime. Let $n \in \mathbb{N}$. Then,

$$\begin{aligned}v_p(n!) &= \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \\ &= \left(n//p^1\right) + \left(n//p^2\right) + \left(n//p^3\right) + \cdots .\end{aligned}$$

Proof. First of all, the infinite sums do make sense, and are actually just finite sums in disguise, meaning that only finitely many of their addends are nonzero.

For instance, if $p = 2$ and $n = 13$, we have

$$\begin{aligned}
&\left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \\
&= \left\lfloor \frac{13}{2^1} \right\rfloor + \left\lfloor \frac{13}{2^2} \right\rfloor + \left\lfloor \frac{13}{2^3} \right\rfloor + \cdots \\
&= \underbrace{\lfloor 6.5 \rfloor}_{=6} + \underbrace{\lfloor 3.25 \rfloor}_{=3} + \underbrace{\lfloor 1.625 \rfloor}_{=1} + \underbrace{\lfloor 0.8125 \rfloor + \lfloor 0.40625 \rfloor + \cdots}_{=0+0+0+\cdots} \\
&= 6 + 3 + 1 + \underbrace{0 + 0 + 0 + \cdots}_{\text{Throw these away}} \\
&= 6 + 3 + 1 = 10.
\end{aligned}$$

Moreover, we know that $\left\lfloor \frac{n}{d} \right\rfloor = n//d$ for any positive integer d. Thus, 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. So we only need to show 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 do this by induction on n:

The *base case* ($n = 0$) is saying that $v_p(1) = 0 + 0 + 0 + \cdots$, which is true since $v_p(1) = 0$.

In the *induction step*, we proceed from $n-1$ to n. So we fix a positive integer n, and assume (as IH) that

$$v_p((n-1)!) = \left\lfloor \frac{n-1}{p^1} \right\rfloor + \left\lfloor \frac{n-1}{p^2} \right\rfloor + \left\lfloor \frac{n-1}{p^3} \right\rfloor + \cdots.$$

Now we must prove that

$$v_p(n!) = \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots.$$

Set $k := v_p(n)$. The factorial recursion says that $n! = (n-1)! \cdot n$. Hence,

$$\begin{aligned}
v_p(n!) &= v_p((n-1)! \cdot n) = v_p((n-1)!) + \underbrace{v_p(n)}_{=k} \\
&= v_p((n-1)!) + k.
\end{aligned}$$

What about the RHSs? Recall the birthday lemma (Corollary 3.3.19 in the notes), we have

$$\left\lfloor \frac{n}{d} \right\rfloor = \begin{cases} \left\lfloor \dfrac{n-1}{d} \right\rfloor + 1, & \text{if } d \mid n; \\ \left\lfloor \dfrac{n-1}{d} \right\rfloor, & \text{if } d \nmid n \end{cases} \qquad \text{for any positive integer } d.$$

Thus,

$$\left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{n-1}{p^i} \right\rfloor + 1 \qquad \text{for any } i \leq k, \qquad \text{and}$$
$$\left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{n-1}{p^i} \right\rfloor \qquad \text{for any } i > k.$$

Hence,

$$\begin{aligned} &\left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \\ &= \left(\left\lfloor \frac{n-1}{p^1} \right\rfloor + 1 \right) + \left(\left\lfloor \frac{n-1}{p^2} \right\rfloor + 1 \right) + \cdots + \left(\left\lfloor \frac{n-1}{p^k} \right\rfloor + 1 \right) \\ &\qquad + \left\lfloor \frac{n-1}{p^{k+1}} \right\rfloor + \left\lfloor \frac{n-1}{p^{k+2}} \right\rfloor + \cdots \\ &= \left(\left\lfloor \frac{n-1}{p^1} \right\rfloor + \left\lfloor \frac{n-1}{p^2} \right\rfloor + \left\lfloor \frac{n-1}{p^3} \right\rfloor + \cdots \right) + k. \end{aligned}$$

Thus, the desired equality

$$v_p(n!) = \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

follows from the IH

$$v_p((n-1)!) = \left\lfloor \frac{n-1}{p^1} \right\rfloor + \left\lfloor \frac{n-1}{p^2} \right\rfloor + \left\lfloor \frac{n-1}{p^3} \right\rfloor + \cdots$$

by adding a k to both sides. □

An application of this lemma is to puzzle questions like "if you write 89! in base-7, how many zeroes are there at the end?". In fact, this question asks for $v_7(89!)$, and this can be computed by the formula we just proved. This can still be used for base-10, even though 10 is not a prime, since $v_{10}(m) = \min\{v_2(m), v_5(m)\}$ for any $m \in \mathbb{Z}$ (why?).

3.6.10. Prime factorization

We are now ready to prove one of the most important properties of primes: the fact that every positive integer can be uniquely decomposed as a product of primes. For instance,

$$200 = 2 \cdot 100 = 2 \cdot 2 \cdot 50 = 2 \cdot 2 \cdot 5 \cdot 10 = \underbrace{2 \cdot 2 \cdot 5 \cdot 5 \cdot 2}_{\text{a product of primes}}.$$

The word "uniquely" means here that any two ways to decompose a given $n > 0$ as a product of primes are equal up to reordering the factors. For instance, 200 is also $2 \cdot 2 \cdot 2 \cdot 5 \cdot 5$, which is the same product but for the order of the primes.

Let us state this fact in full generality:

Definition 3.6.14. Let n be a positive integer. A **prime factorization** of n means a finite list $(p_1, p_2, \ldots, p_k)$ of primes (not necessarily distinct) such that

$$n = p_1 p_2 \cdots p_k.$$

For example, $(2, 2, 5, 2, 5)$ and $(5, 2, 2, 5, 2)$ are two prime factorizations of 200. Now our claim is:

Theorem 3.6.15 (Fundamental Theorem of Arithmetic)**.** Let n be a positive integer. Then:

(a) There exists a prime factorization of n.

(b) This prime factorization is unique up to reordering its entries. In other words, if $(p_1, p_2, \ldots, p_k)$ and $(q_1, q_2, \ldots, q_\ell)$ 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 the list $(p_1, p_2, \ldots, p_k)$ is $v_p(n)$.

Proof. **(a)** We proved this as an example of strong induction.

(c) We have $n = p_1 p_2 \cdots p_k$. Thus,

$$\begin{aligned}
v_p(n) &= v_p(p_1 p_2 \cdots p_k) \\
&= v_p(p_1) + v_p(p_2) + \cdots + v_p(p_k) \qquad \text{(by the last corollary above)} \\
&= \left(\begin{array}{c} \text{a sum of 0's and 1's, which contains as many 1's} \\ \text{as there are } p_i\text{'s equal to } p \end{array} \right) \\
&\qquad \left(\text{since } v_p(p) = 1 \text{ and } v_p(q) = 0 \text{ for any prime } q \neq p\right) \\
&= (\text{the number of 1's in this sum}) \\
&= (\text{the number of } p_i\text{'s equal to } p) \\
&= (\text{the number of times } p \text{ appears in } (p_1, p_2, \ldots, p_k)).
\end{aligned}$$

(b) Let $(p_1, p_2, \ldots, p_k)$ and $(q_1, q_2, \ldots, q_\ell)$ be two prime factorizations of n. Then, for any prime p, the number of times that p appears in $(p_1, p_2, \ldots, p_k)$ equals $v_p(n)$ (by part **(c)**), but the number of times that p appears in $(q_1, q_2, \ldots, q_\ell)$ also equals $v_p(n)$. Thus, p appears the same number of times in both lists.

So we have shown that the two lists contain each prime the same number of times. So they have the same entries, just in a different order. Qed. □

3.7. Least common multiples

We have studied greatest common divisors above. Least common multiples are some kind of counterpart to them: Given two integers a, b, the gcd of a and b is the (nonnegative) common divisor of a and b that is divisible by all common divisors of a and b, whereas the lcm (= least common multiple) of a and b is the (nonnegative) common multiple of a and b that divides all common multiples of a and b. Let us explain this in more detail.

Definition 3.7.1. Let a and b be two integers.

(a) The **common multiples** of a and b are the integers that are divisible by both a and b simultaneously.

(b) The **least common multiple** of a and b (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 $\operatorname{lcm}(a, b)$.

Examples:

- We have $\operatorname{lcm}(3, 4) = 12$.
- We have $\operatorname{lcm}(6, 4) = 12$.
- We have $\operatorname{lcm}(6, 8) = 24$.

  (The positive multiples of 8 are 8, 16, 24, ... You can check that the first of these to be a multiple of 6 is 24.)
- We have $\operatorname{lcm}(3, 6) = 6$.
- We have $\operatorname{lcm}(0, 3) = 0$ by definition.
- We have $\operatorname{lcm}(3, -4) = 12$. In fact, the multiples of -4 are precisely the multiples of 4, since divisibility does not depend on the sign.

Note that the lcm of two (or more) positive integers is important for working fractions: If you have several fractions with integer denominators, then the lcm of these denominators is exactly the least (= lowest) common denominator that you can use to add these fractions together.

Let us study some basic properties of lcms:

Theorem 3.7.2. Let a and b be two integers. Then:
(a) The lcm of a and b exists.
(b) We have $\operatorname{lcm}(a,b) \in \mathbb{N}$.
(c) We have $\operatorname{lcm}(a,b) = \operatorname{lcm}(b,a)$.
(d) We have $a \mid \operatorname{lcm}(a,b)$ and $b \mid \operatorname{lcm}(a,b)$.
(e) We have $\operatorname{lcm}(-a,b) = \operatorname{lcm}(a,b)$ and $\operatorname{lcm}(a,-b) = \operatorname{lcm}(a,b)$.

Proof. **(a)** If a or b is 0, then this is true by definition. Otherwise, $|ab|$ is a positive common multiple of a and b. So there is a smallest positive common multiple of a and b. In other words, $\operatorname{lcm}(a,b)$ exists.
(b), **(c)**, **(d)** Obvious from the definition.
(e) This is because divisibility does not care about the sign. □

Now, a universal property. Recall the universal property of the gcd, which says that

$$(m \mid a \text{ and } m \mid b) \iff (m \mid \gcd(a,b)).$$

Here is an analogous property for the lcm:

Theorem 3.7.3 (universal property of the lcm)**.** Let $a, b, m \in \mathbb{Z}$. Then, we have the equivalence

$$(a \mid m \text{ and } b \mid m) \iff (\operatorname{lcm}(a,b) \mid m).$$

Proof. $\Longleftarrow$: If $\operatorname{lcm}(a,b) \mid m$, then $a \mid m$ (because $a \mid \operatorname{lcm}(a,b) \mid m$) and similarly $b \mid m$.

$\Longrightarrow$: Assume that $a \mid m$ and $b \mid m$. We must prove that $\operatorname{lcm}(a,b) \mid m$.

If one of a and b is 0, then this is easy (since $a \mid m$ and $b \mid m$ imply that $m = 0$ in this case, and thus m is divisible by $\operatorname{lcm}(a,b)$).

So we only need to consider the case when a and b are nonzero. In this case, set $\ell = \operatorname{lcm}(a,b)$. Then, ℓ is the smallest positive common multiple of a and b (by definition). Hence, ℓ is a positive integer and is a multiple of a and of b. Our goal is to prove that $\ell \mid m$.

Set $q := m//\ell$ and $r := m\%\ell$ be the quotient and the remainder obtained when dividing m by ℓ. Thus,

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

Hence, $r < \ell$.

From $m = q\ell + r$, we obtain $r = m - q\ell$. Since both m and ℓ are multiples of a (since $a \mid m$ and $\ell = \operatorname{lcm}(a,b)$), we thus concldue that r is a multiple of a as well. Similarly, r is a multiple of b. So r is a common multiple of a and b. If r was positive, then this would be absurd, since ℓ is the smallest positive common multiple of a and b but r is smaller ($r < \ell$). So r cannot be positive. But $r \in \{0, 1, \ldots, \ell - 1\}$. Thus, $r = 0$. Hence, $m\%\ell = r = 0$, so that $\ell \mid m$, qed. □

The gcd and the lcm of two integers are related to each other by the following formula:

Theorem 3.7.4. Let a and b be two integers. Then,

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|.$$

Proof sketch. The case when a or b is 0 is easy. So let us consider the other case. Here, argue that $\dfrac{ab}{\gcd(a,b)}$ is a common multiple of a and b, and thus (by the universal property) is a multiple of $\operatorname{lcm}(a,b)$. Thus, ab is a multiple of $\gcd(a,b) \cdot \operatorname{lcm}(a,b)$.

On the other hand, argue that $\dfrac{ab}{\operatorname{lcm}(a,b)}$ is an integer and divides $\gcd(a,b)$ (since it divides each of a and b). Thus, ab divides $\gcd(a,b) \cdot \operatorname{lcm}(a,b)$.

Now recall that if two integers x and y are mutual multiples (i.e., we have $x \mid y$ and $y \mid x$), then $|x| = |y|$. Conclude.

(Details in a reference in the notes.) □

Both gcds and lcms have easily computable p-valuations:

Theorem 3.7.5. Let p be a prime. Let a and b be two integers. Then,

$$v_p(\gcd(a,b)) = \min\left\{v_p(a),\ v_p(b)\right\};$$
$$v_p(\operatorname{lcm}(a,b)) = \max\left\{v_p(a),\ v_p(b)\right\}.$$

Proof. Not hard using the properties of p-valuations and the universal properties of gcd and lcm. (See the notes for a reference.) □

This theorem is useful for computing $\gcd(a,b)$ and $\operatorname{lcm}(a,b)$ if you know the prime factorizations of two integers a and b. For example, knowing that $18 = 2^1 \cdot 3^2$ and $12 = 2^2 \cdot 3^1$, we obtain

$$\gcd(18,\ 12) = 2^1 \cdot 3^1 = 2 \cdot 3 = 6 \qquad \text{and}$$
$$\operatorname{lcm}(18,\ 12) = 2^2 \cdot 3^2 = 36.$$

If you don't know the prime factorizations, it is easiest to compute $\gcd(a,b)$ by the Euclidean algorithm and then compute $\operatorname{lcm}(a,b)$ by solving the equation

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|.$$

Gcds and lcms can also be defined for more than two numbers. Most of the above properties still hold, except that the formula

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|$$

becomes more complicated (it is 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 most texts on elementary number theory, or my 2019 notes (referenced in the notes).

3.8. Sylvester's $xa + yb$ theorem (or the Chicken McNugget theorem)

We make a little digression to state a theorem about the coin problem we have discussed a while ago: What denominations can be paid using a-cent coins and b-cent coins (without change).

For this little section, we let a and b be two positive integers.

Definition 3.8.1. (a) A **$\mathbb{Z}$-linear combination** (or **$\mathbb{Z}$-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 can be paid using a-cent coins and b-cent coins if you can get change.

(b) An **$\mathbb{N}$-linear combination** (or **$\mathbb{N}$-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 can be paid using a-cent coins and b-cent coins if you cannot get change.

Back in the "strong induction" section, we showed that any integer $n \geq 8$ is an $\mathbb{N}$-LC of 3 and 5. More concretely, the $\mathbb{N}$-LCs of 3 and 5 are

$$0,\ 3,\ 5,\ 6,\ \underbrace{8,\ 9,\ 10,\ \ldots}_{\text{all integers } \geq 8}.$$

This should make us wonder what we can say about the $\mathbb{N}$-LCs of a and b in the general case. We shall begin with describing the $\mathbb{Z}$-LCs, since this is easier. Any $\mathbb{N}$-LC is a $\mathbb{Z}$-LC. However, a $\mathbb{Z}$-LC is not always an $\mathbb{N}$-LC (for example, 1 is a $\mathbb{Z}$-LC of 3 and 5, but not an $\mathbb{N}$-LC).

Proposition 3.8.2. The $\mathbb{Z}$-LCs of a and b are exactly the multiples of $\gcd(a,b)$.

Proof idea. Any $\mathbb{Z}$-LC of a and b is a multiple of $\gcd(a,b)$, since it can be written as $xa+yb$ and you can factor a $\gcd(a,b)$ out of this sum.

Conversely, any multiple of $\gcd(a,b)$ is a $\mathbb{Z}$-LC of a and b, since Bezout's theorem yields that $\gcd(a,b)$ itself is one.

(See the notes for more details.) □

What can we say about the $\mathbb{N}$-LCs? A more complicated example:

The $\mathbb{N}$-LCs of 5 and 9 are

$$0,\ 5,\ 9,\ 10,\ 14,\ 15,\ 18,\ 19,\ 20,\ 23,\ 24,\ 25,\ 27,\ 28,\ 29,\ 30,\ \underbrace{32,\ 33,\ 34,\ \ldots}_{\text{all integers } \geq 32}.$$

We do not expect to have an explicit way of describing them all. But we can notice a few things: All integers $\geq$ some threshold are $\mathbb{N}$-LCs of 5 and 9, and moreover, exactly half the integers below this threshold are.

These patterns generalize! All you have to require is that a and b are coprime. (This is not a very stringent requirement, because the non-coprime case can be reduced to the coprime case by replacing a and b with $a/\gcd(a,b)$ and $b/\gcd(a,b)$.) The result is:

Theorem 3.8.3 (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 $(a-1)(b-1)$ nonnegative integers

$$0,\ 1,\ 2,\ \ldots,\ ab-a-b,$$

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 $ab-a-b$ is an $\mathbb{N}$-LC of a and b.

See the notes for a proof. (This theorem was found by J. J. Sylvester in 1884.)

3.9. An introduction to cryptography

This is a digression; this material is not examinable. Cryptography is a wide field (not really a part of mathematics, but relying on a lot of mathematics) and has its own courses here at Drexel. Let me briefly survey a couple highlights from classical and modern cryptography.

Cryptography is the study of ciphers – i.e., ways to encrypt data. Data, for us, is text.

We will see an ancient (Roman) as well as a modern (20th century) cipher. Both rely on number theory. There are many more ciphers, and a bunch of books discussing them, some referenced in the notes.

3.9.1. Caesarian ciphers (alphabet rotation)

We start with an algorithm that was used by Julius Caesar to encrypt military communications. We assume that our messages are written in the modern Latin alphabet, all-uppercase.

The modern Latin alphabet has 26 letters: A, B, ..., Z. We assign a number to each letter:

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 $\sim$ 5 and X $\sim$ 23. This method of encoding letters as numbers will be called **numerical encoding**.

A word is just a finite list of letters, and thus can be encoded as a finite list of numbers: e.g.,

$$\text{KITTEN} \ \to \ (\text{K, I, T, T, E, N}) \to (10,\ 8,\ 19,\ 19,\ 4,\ 13)\,.$$

Conversely, any list of numbers in $\{0, 1, \ldots, 25\}$ can be decoded into a word. For instance, $(17,\ 0,\ 19) \to (\text{R, A, T}) \to \text{RAT}$.

With these bases covered, we can now formulate Caesar's algorithm for encrypting a word. This 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 $(a_1, a_2, \ldots, a_n)$.
2. Replace each number a_i by $(a_i + 3)\,\%26$.
3. Decode the resulting list back into a word.

For instance,

$$\text{CRAZY} \ \to \ (2,\ 17,\ 0,\ 25,\ 24) \to (5,\ 20,\ 3,\ 2,\ 1) \to \text{FUDCB}.$$

In other words, the Caesarian cipher ROT_3 simply shifts each letter by 3 forward, if you consider the letters of the alphabet as being wrapped around a circle.

How can we decrypt a word encrypted using ROT_3 ? By shifting each letter by 3 backward, i.e., replacing each a_i by $(a_i - 3)\,\%26$. We can denote this operation by ROT_{-3}.

More generally, we define ROT_k for any integer k as follows:

Caesarian cipher ROT_k**:** Let k be a fixed integer. To encrypt a word, proceed as follows:

1. Encode the word as a finite list of numbers $(a_1, a_2, \ldots, a_n)$.
2. Replace each number a_i by $(a_i + k)\,\%26$.
3. Decode the resulting list back into a word.

In other words, ROT_k shifts each letter by k steps forward. It is easy to see that a word encrypted using ROT_k can be decrypted back using ROT_{-k}. This relies on the following simple lemma:

Lemma 3.9.1. Let $a, b \in \{0, 1, \ldots, 25\}$ be such that $b = (a + k)\,\%26$. Then, $a = (b - k)\,\%26$.

Proof. From $b = (a + k)\,\%26$, we have $b \equiv a + k \bmod 26$. Hence, $b - k \equiv a \bmod 26$, that is, $a \equiv b - k \bmod 26$. Therefore, $a = (b - k)\,\%26$ (since $a \in \{0, 1, \ldots, 25\}$). □

Some observations:

- The encryption method ROT_0 does nothing: Each word is encrypted as itself.
- The encryption method ROT_{26} also does nothing: Each word is encrypted as itself.
- The encryption method ROT_{27} does the same as ROT_1.
- More generally, if $u \equiv v \bmod 26$, then $\mathrm{ROT}_u = \mathrm{ROT}_v$.
- So the only Caesarian ciphers are

  $$\mathrm{ROT}_0,\ \mathrm{ROT}_1,\ \ldots,\ \mathrm{ROT}_{25}.$$

  Any other ROT_k is just a copy of one of these. Of these 26 ciphers, only 25 are useful, since ROT_0 does nothing.
- The cipher ROT_{13} is self-inverse: Decrypting a word encrypted using ROT_{13} can be done using ROT_{13} again. Indeed, ROT_{13} is undone by ROT_{-13}, but $\mathrm{ROT}_{-13} = \mathrm{ROT}_{13}$ because $-13 \equiv 13 \bmod 26$.
- Encoding a word using ROT_a and then encoding the result using ROT_b is the same as encoding the original word using ROT_{a+b}.

3.9.2. Keys and ciphers

Ciphers such as ROT_k are one-trick ponies: Once your enemy knows the method, he will be able to decrypt anything you encrypt.

This is true to an extent even if the enemy does **not** know the k. Indeed, there are only 26 Caesarian ciphers

$$\mathrm{ROT}_0,\ \mathrm{ROT}_1,\ \ldots,\ \mathrm{ROT}_{25}\,.$$

Thus, if your enemy finds a text you encrypted using some ROT_k, he can just try to decrypt it using

$$\mathrm{ROT}_{-0},\ \mathrm{ROT}_{-1},\ \ldots,\ \mathrm{ROT}_{-25},$$

and see which of the results gives a meaningful word/text.

In modern language, this is saying that Caesarian ciphers have too small a key length.

Example: BPQA QA VWB BPM EIG

Try to apply every ROT_k. You find that ROT_{18} gives "THIS IS NOT THE WAY", which is valid text. So the text was ROT_{-18}-encrypted, i.e., ROT_8-encrypted.

So how can we create a cipher that is harder to break? We need a bigger key size, and we need "more chaos" (e.g., don't apply the same rule to each letter). Here are some ciphers that are slightly better in some of these regards:

- **Monoalphabetic substitution:** Here we still do the same thing to each letter, but the thing is no longer just a shift by k letters. Instead, we fix **any** permutation of the alphabet (i.e., a rule that sends each letter to a different letter) and we apply this permutation separately to each letter. For instance, we can use the following permutation:

A	B	C	D	E	F	G	H	I	J	K	L	M
C	Z	X	B	N	M	P	A	D	T	S	R	Q

.

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
K	O	E	W	Y	U	I	J	F	L	G	H	V

  For example, the word KITTEN is then encrypted as SDIINK.

  The key size of this encryption method is huge – it is the number of all permutations of the alphabet, which is (as we will soon see) $26! = 403\,291\,461\,126\,605\,635\,584\,000\,000$. You cannot just try all these keys manually. But you can exploit certain patterns in the English language (or whatever language the text is written it), such as frequencies of letters, frequencies of two-letter combinations, and so on.

- **Viginere substitution:** Now the key is a very long sequence

$$(b_1, b_2, b_3, \ldots)$$

of elements of $\{0, 1, \ldots, 25\}$ (or just of integers). To encrypt a word, we first encode it as a tuple of integers $(a_1, a_2, \ldots, a_n)$, and then replace each number a_i by $(a_i + b_i)$ %26; then, the resulting tuple is decoded back into a word.

This is essentially a generalized Caesarian cipher, in which we let each letter get a different key depending on its position. This cipher is completely unbreakable, however it is very inconvenient: You need an infinitely long key (or at least a key longer than the text you want to encrypt). Such keys are historically known as **codebooks**. The codebook contains the numbers $b_1, b_2, b_3, \ldots$, and must be at least as long as the total text you want to encrypt.

In many cases, this becomes impractical, so people have tried to "cheat", e.g., by using a periodic sequence $(b_1, b_2, b_3, \ldots)$, the cipher becomes breakable when the ciphertext is sufficiently long.

Many different algorithms have been found over the ages, usually striking some balance between practicality (ease of use, simplicity, shortness of the key) and security (unbreakability). See, e.g., Simon Singh's "Code book" for some history and examples.

3.9.3. The RSA cipher

All ciphers until the early 20th century are **classical ciphers** – they are supposed to be encryptable and decryptable without the use of computers or particularly complicated tools. The 20th century saw computers and thus a huge speedup of computations. This made almost all classical ciphers breakable. In fact, some of the oldest computers were built to break ciphers.

Modern ciphers are ciphers that require a computer to encrypt and decrypt. No one knows for sure whether they are breakable, but at least in many cases we have good reason to suspect that they are not, at least not on the hardware we have currently. One such cipher is the **RSA cipher**, developed by Rivest, Shamir and Adleman in the 1970s/80s.

Like any modern cipher, the RSA cipher works on digital data. It addresses a fairly standard situation: Albert and Julia are communicating over a channel (e.g., the Internet), but the channel may have eavesdroppers, so their communication is not private. Julia wants to send a secret message to Albert over the channel – i.e., a message that eavesdroppers should not be able to decipher. But Albert and Julia have not exchanged keys with each other in advance. If they start exchanging keys now, the eavesdropper will obviously learn these keys as well! Can Albert and Julia still communicate securely?

Surprisingly, the answer is "yes". Here is how this works (per the RSA cipher):

Setup:

- Julia tells Albert 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? There is a lot of skill involved in here. For example, there are prime number tests – i.e., methods to check if a given number is prime. What does "sufficiently random" mean? Not clear, but there are several good ways to get something "practically random".]
- Albert computes the positive integer $m := pq$. This number m (called the **modulus**) he makes public (i.e., sends to Julia). Eavesdroppers will thus learn m but will probably struggle finding p and q because it is hard to factor numbers into primes.
- Albert also computes the positive integer $\ell := (p-1)(q-1)$, but keeps it private.
- Albert randomly picks an $e \in \{2, 3, \ldots, \ell - 1\}$ that is coprime to ℓ.

  [Again, how? Actually, picking a bunch of numbers at random will quickly give you one that is coprime to ℓ. Coprimality can be checked quickly using the Euclidean algorithm.]
- Albert computes a positive integer d such that $ed \equiv 1 \bmod \ell$.

  [How? Bezout's theorem (and the extended Euclidean algorithm) show that $1 = \gcd(e, \ell) = xe + y\ell$ for some $x, y \in \mathbb{Z}$. So $1 = xe + y\ell \equiv xe = ex \bmod \ell$ and therefore $ex \equiv 1 \bmod \ell$. So we 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 it is m or larger, we just break it up into size-m chunks and encrypt each chunk separately.)

Encrypting a message:

If Julia wants to send a message $a \in \{0, 1, \ldots, m-1\}$ to Albert, then she does the following:

She computes $a^e \% m$ and sends that to Albert.

So the encryption algorithm is just "take the e-th power and then take its remainder when divided by m".

[In practice, you don't have to compute a^e to get to the remainder. Instead, you can take powers "in $\{0, 1, \ldots, m-1\}$" by taking a remainder every time you "overflow" this set. For instance, to compute $a^3 \% m$, you can compute $\left(\left(a^2 \% m\right) a\right) \% m$. This way you never have to deal with integers larger than m^2. Even better, you can use binary exponentiation, for example $a^4 = \left(a^2\right)^2$ and $a^4 \% m = \left(a^2 \% m\right)^2 \% m$.]

Decrypting a message:
Albert receives the remainder $b = a^e \% m$. To recover the original message a, he just needs to take the d-th power and take its remainder upon division by m. In other words,

$$a = b^d \% m.$$

Why does this work? Obviously, we need to prove the following proposition:

Proposition 3.9.2 (correctness of RSA)**.** Let p and q be two distinct primes. Let $m = pq$ and $\ell = (p-1)(q-1)$. Let e be a positive integer coprime to m, and let d be a positive integer such that $ed \equiv 1 \bmod \ell$.

Let a and b be two numbers in $\{0, 1, \ldots, m-1\}$ such that $b = a^e \% m$. Then, $a = b^d \% m$.

This is not at all obvious! The RSA cipher might resemble a Caesarian cipher in that we are using remainders, but it is different in that it takes powers instead of adding/subtracting a fixed k.

To prove the proposition, we will need a lemma:

Lemma 3.9.3. Let p and q be two distinct primes. Let N be a positive integer such that $N \equiv 1 \bmod (p-1)(q-1)$. Then, for every integer a, we have

$$a^N \equiv a \bmod pq.$$

Proof. Fermat's little theorem says that $a^p \equiv a \bmod p$ and $a^q \equiv a \bmod q$. Our claim looks similar, but not quite the same.

We must prove that $a^N \equiv a \bmod pq$. In other words, we must prove $pq \mid a^N - a$. But p and q are two distinct primes, and thus are coprime (why?), so that $pq \mid a^N - a$ would follow from $p \mid a^N - a$ and $q \mid a^N - a$ (by the coprime divisors theorem).

So we only need to prove $p \mid a^N - a$ and $q \mid a^N - a$. We will only show $p \mid a^N - a$, since $q \mid a^N - a$ is analogous.

In other words, we must show that $a^N \equiv a \bmod p$.

Recall that $N \equiv 1 \bmod (p-1)(q-1)$, so that $N \equiv 1 \bmod p - 1$ (by the rule that $a \equiv b \bmod c$ always implies $a \equiv b \bmod d$ whenever $d \mid c$). In other words, $p - 1 \mid N - 1$, so that $N - 1 = (p-1)c$ for some integer c. Easily, $c \geq 0$. Thus,

$$N = 1 + (p-1)c,$$

so

$$\begin{aligned} a^N &= a^{1+(p-1)c} = a\,\underbrace{a^{p-1}a^{p-1}a^{p-1}\cdots a^{p-1}}_{c \text{ times}} \\ &= \underbrace{aa^{p-1}}_{\substack{=a^p \equiv a \bmod p \\ \text{(by Fermat)}}} \underbrace{a^{p-1}a^{p-1}\cdots a^{p-1}}_{c-1 \text{ times}} \\ &\equiv a\,\underbrace{a^{p-1}a^{p-1}\cdots a^{p-1}}_{c-1 \text{ times}} \\ &\equiv a\,\underbrace{a^{p-1}a^{p-1}\cdots a^{p-1}}_{c-2 \text{ times}} \\ &\equiv \cdots \\ &\equiv a \bmod p. \end{aligned}$$

So $p \mid a^N - a$, and this completes the proof of the lemma. □

Example 3.9.4. Let us apply the lemma to $p = 3$ and $q = 5$ and $N = 9$. Then, the lemma says that

$$a^9 \equiv a \bmod 15 \qquad \text{for every integer } a.$$

Proof of the proposition. From $b = a^e \% m \equiv a^e \bmod m$. Taking this congruence to the d-th power, we obtain

$$b^d \equiv \left(a^e\right)^d = a^{ed} \bmod m.$$

But $ed \equiv 1 \bmod \ell$, that is, $ed \equiv 1 \bmod (p-1)(q-1)$. Hence, the lemma (applied to $N = ed$) yields

$$a^{ed} \equiv a \bmod pq, \qquad \text{that is,} \qquad a^{ed} \equiv a \bmod m.$$

So

$$b^d \equiv a^{ed} \equiv a \bmod m.$$

Therefore, $b^d \% m = a \% m = a$ (since $a \in \{0, 1, \ldots, m-1\}$), qed. □

The above method lets Julia send secret messages to Albert. If Albert wants to respond secretly, the two have to switch roles (i.e., now Julia must set up her two primes p' and q', her m', ℓ', e' and d', publish her public key (e', m'), and let Albert encrypt his message using that public key).

The RSA cipher is not hard to implement in your favorite programming language, provided that it has sufficiently big integers. But there are some practical considerations:

- You want sufficiently random primes. (Generally, any cipher requires something sufficiently random that the eavesdroppers cannot guess.)
- Certain primes are bad choices of p and q, since they allow certain tricks for computing d. You want to avoid such primes.
- You want to avoid certain practical "side channels".
- You don't want your a to be much smaller than m. If it is, pad it with random bits.

The RSA cipher can be used not just for encrypting secret messages, but also for authentification (i.e., proving that a message is really coming from you).

More modern technologies like elliptic curve cryptography are harder to get wrong, but also more complicated. In a way, elliptic curve cryptography uses "the same idea" but more complicated objects than remainders upon division by m.

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 some counting problems:

- How many ways are there to choose 3 odd integers between 0 and 20, if the order matters (i.e., we count the choice $1, 3, 5$ as different from $3, 1, 5$) ? The answer is 1000.
- 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? (We count different orderings as distinct.) The answer is 10.
- How many ways are there to tile a 2×15-rectangle with dominos (i.e., rectangles of size 1×2 or 2×1)? The answer is 987.
- How many addends do you get when you expand the product $(a + b)(c + d + e)(f + g)$? The answer is 12.

- How many positive divisors does 24 have? These are 1, 2, 3, 4, 6, 8, 12, 24, so the answer is 8.

In the rest of this quarter, we will solve some of these problems and some more. First, we will solve some of these problems informally; then we will make the concepts rigorous using the notion of a **function**, and come back to solve the rest.

4.1. A refresher on sets

You have encountered sets in a prerequisite course, so this will be brief and mostly introduce notations.

Informally, a **set** is a collection of objects. It knows which objects it contains and which it does not.

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., contain nothing) or nonempty (i.e., contain some element).

An example of a set is the set of all odd integers. It contains every odd integer and nothing else. Generally, "the set of X" means the set that contains X and nothing else.

A finite set can be written by listing all its elements. For example, the set of all odd integers between 0 and 10 can be written as

$$\{1,3,5,7,9\}.$$

The braces $\{$ and $\}$ around the list are signalling that we are taking the set of the elements listed between them. These braces are called "set braces", and can be used not only with lists inside.

Some more examples of finite sets are

$$\begin{aligned}
&\{1,2,3,4,5\},\\
&\{1,2\},\\
&\{1\} \qquad (\text{this is the set that only contains } 1),\\
&\{\} \qquad (\text{the empty set, also denoted } \varnothing),\\
&\{1,2,\ldots,1000\} \qquad \left(\begin{array}{c}\text{the "}\ldots\text{" here is understood to}\\ \text{be clear from the context}\end{array}\right).
\end{aligned}$$

Some infinite sets can also be written in this form:

$$\begin{aligned}
&\{1,2,3,\ldots\} && \text{(this is the set of all positive integers)},\\
&\{0,1,2,\ldots\} && \text{(this is the set of all nonnegative integers)},\\
&\{-1,-2,-3,\ldots\} && \text{(this is the set of all negative integers)},\\
&\{\ldots,-2,-1,0,1,2,\ldots\} && \text{(this is the set of all integers)}.
\end{aligned}$$

Some others cannot. For example, it would be very hard to write the set of all rational numbers this way.

Another way to describe a set is just by putting a description of its elements in set braces. For example,

$$\begin{aligned}
&\{\text{all integers}\} && \text{(this is the set of all integers)},\\
&\{\text{all nonnegative integers}\},\\
&\{\text{all integers between 3 and 9 inclusive}\},\\
&\{\text{all real numbers}\}.
\end{aligned}$$

Often, you want to define a set that contains all things of a certain type that satisfy a certain condition. For example, you might want the set of all integers x such that $x^2 < 20$. This is written as

$$\left\{x \text{ is an integer } \mid\ x^2 < 20\right\}.$$

The vertical bar $\mid$ here should be read as "such that" (do not mistake it for the identical-looking divisibility bar or absolute-value bracket). The part before this bar tells you what types of things you are putting in the set (here, the integers x); the part after this bar poses conditions under which they go into the set (here, $x^2 < 20$). The notation then signifies the set of all things of the former type that satisfy the latter conditions. For instance,

$$\begin{aligned}
&\left\{x \text{ is an integer } \mid\ x^2 < 20\right\}\\
&= \{\text{all integers whose squares are smaller than } 20\}\\
&= \{-4,-3,-2,-1,0,1,2,3,4\}.
\end{aligned}$$

Sometimes, a colon : is written instead of $\mid$.

Some sets have standard names:

$$\begin{aligned}
\mathbb{N} &= \{\text{all nonnegative integers}\} = \{0,1,2,\ldots\};\\
\mathbb{Z} &= \{\text{all integers}\} = \{\ldots,-2,-1,0,1,2,\ldots\};\\
\mathbb{Q} &= \{\text{all rational numbers}\};\\
\mathbb{R} &= \{\text{all real numbers}\};\\
\mathbb{C} &= \{\text{all complex numbers}\}.
\end{aligned}$$

For us, $\mathbb{N}$ and $\mathbb{Z}$ are the most useful.

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 example,

$$\left\{x^2 + 2 \mid\ x \in \{1,3,5,7,9\}\right\}$$

means the set whose elements are the numbers $x^2 + 2$ for all $x \in \{1,3,5,7,9\}$. Thus,

$$\begin{aligned}&\left\{x^2 + 2 \mid\ x \in \{1,3,5,7,9\}\right\}\\ &= \left\{1^2 + 2,\ 3^2 + 2,\ 5^2 + 2,\ 7^2 + 2,\ 9^2 + 2\right\}\\ &= \{3,\ 11,\ 27,\ 51,\ 83\}.\end{aligned}$$

In general, if S is a given set, then

$$\{\text{an expression} \mid\ x \in S\}$$

means the set whose elements are the values of the given expression for all $x \in S$.

Some more examples:

$$\begin{aligned}&\left\{\frac{x+1}{x} \mid\ x \in \{1,2,3,4\}\right\}\\ &= \left\{\frac{1+1}{1}, \frac{2+1}{2}, \frac{3+1}{3}, \frac{4+1}{4}\right\}\\ &= \left\{2, \frac{3}{2}, \frac{4}{3}, \frac{5}{4}\right\}.\end{aligned}$$

Also,

$$\begin{aligned}&\left\{x^2\%5 \mid\ x \in \mathbb{N}\right\}\\ &= \left\{0^2\%5,\ 1^2\%5,\ 2^2\%5,\ 3^2\%5,\ 4^2\%5,\ \ldots\right\}\\ &= \{0,\ 1,\ 4,\ 4,\ 1,\ 0,\ 1,\ \ldots\}.\end{aligned}$$

The remainders $x^2\%5$ repeat every five steps (since each $x \in \mathbb{Z}$ satisfies $x^2 \equiv (x+5)^2 \bmod 5$), and thus the only values are 0, 1 and 4. So

$$\left\{x^2\%5 \mid\ x \in \mathbb{N}\right\} = \{0,1,4\}.$$

Let me stress once again that a set knows neither the order of its elements, nor "how often" they appear. In particular,

$$\{1,2\} = \{2,1\} = \{1,2,1\} = \{1,1,2\} = \{2,1,2,1,2,1\}\,.$$

Sets can be combined and compared in many ways:

Definition 4.1.1. Let A and B be two sets.

(a) We say that A is a **subset** of B (and we write $A \subseteq B$) if every element of A is an element of B.

(b) We say that A is a **superset** of B (and we write $A \supseteq B$) if every element of B is an element of A. This is equivalent to $B \subseteq A$.

(c) We say that $A = B$ if the sets A and B contain the exact same elements. This is tantamount to saying that $A \subseteq B$ 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

$$\begin{aligned} A \setminus B &:= \{\text{all elements that are contained in } A \text{ but not in } B\} \\ &= \{x \mid x \in A \text{ and } x \notin B\} = \{x \in A \mid x \notin B\}\,. \end{aligned}$$

This is denoted by $A - B$ by some authors.

(g) We say that A and B are **disjoint** if $A \cap B = \varnothing$ (that is, A and B have no element in common).

For example,

$$\begin{aligned} \{2,4,6\} &\subseteq \{1,2,3,4,5,6\}\,, \\ \{1,2,3,4,5,6\} &\supseteq \{2,4,6\}\,, \\ \text{we } \textbf{don't} \text{ have } \{5,6,7\} &\subseteq \{1,2,3,4,5,6\}\,, \\ \{1,2,3\} &= \{3,2,1\}\,, \\ \{1,3,5\} \cup \{3,6\} &= \{1,3,5,3,6\} = \{1,3,5,6\}\,, \\ \{1,3,5\} \cap \{3,6\} &= \{3\}\,, \\ \{1,2,4\} \cap \{3,5\} &= \varnothing, \qquad \text{so the sets } \{1,2,4\} \text{ and } \{3,5\} \text{ are disjoint,} \\ \{1,3,5\} \setminus \{3,6\} &= \{1,5\}\,, \\ \mathbb{Z} \setminus \mathbb{N} &= \{\text{all negative integers}\} = \{-1,-2,-3,\ldots\}\,. \end{aligned}$$

Definition 4.1.2. Several sets $A_1, A_2, \ldots, A_k$ are said to be **disjoint** if any two of them are disjoint (not counting a set and itself), i.e., if we have

$$A_i \cap A_j = \varnothing \qquad \text{for all } i < j.$$

For example, the three sets $\{1,5\}$, $\{2,6\}$ and $\{3\}$ are disjoint, but the three sets $\{1,5\}$, $\{2,6\}$ and $\{3,5\}$ are not (since $\{1,5\} \cap \{3,5\} \neq \varnothing$).

4.2. Counting, informally

We will now see how the elements of a set can be counted. We will define "counting" formally later (next week?), but for now let us use our common sense and see what we can say.

For example, the set of all odd integers between 0 and 10 has 5 elements: 1, 3, 5, 7, 9.

More generally, I claim:

Proposition 4.2.1. Let $n \in \mathbb{N}$. Then, there are exactly $(n+1)\,//\,2 = \left\lfloor \dfrac{n+1}{2} \right\rfloor$ odd integers between 0 and n (inclusive).

Informal proof. The equality $(n+1)\,//\,2 = \left\lfloor \dfrac{n+1}{2} \right\rfloor$ follows from something we did long ago ($n//d = \left\lfloor \dfrac{n}{d} \right\rfloor$). It remains to prove that there are exactly $\left\lfloor \dfrac{n+1}{2} \right\rfloor$ odd integers between 0 and n.

Let us prove this by induction on n:

Base case: We must prove this claim for $n = 0$. This is saying that there are exactly $\left\lfloor \dfrac{0+1}{2} \right\rfloor$ odd integers between 0 and 0. This is just saying $0 = 0$.

Induction step: Let n be a positive integer. Assume (as the IH) that the claim is true for $n-1$. That is, assume that there are exactly $\left\lfloor \dfrac{n}{2} \right\rfloor$ odd integers between 0 and $n-1$. In other words, assume that

$$(\#\text{ of odd integers between 0 and } n-1) = \left\lfloor \frac{n}{2} \right\rfloor.$$

(Here and in the following, the symbol "#" means "number".)

Our goal is to prove that

$$(\#\text{ of odd integers between 0 and } n) = \left\lfloor \frac{n+1}{2} \right\rfloor.$$

We are in one of the following two cases:

Case 1: The number n is even.

Case 2: The number n is odd.

Consider Case 1. Here, n is even. Thus, n is not odd. Therefore, the odd integers between 0 and n are precisely the odd integers between 0 and $n-1$. Hence,

$$\begin{aligned}
&(\#\text{ of odd integers between 0 and } n) \\
&= (\#\text{ of odd integers between 0 and } n-1) \\
&= \left\lfloor \frac{n}{2} \right\rfloor \qquad (\text{by the IH}) \\
&= \left\lfloor \frac{n+1}{2} \right\rfloor \qquad (\text{since } n \text{ is even}).
\end{aligned}$$

This proves the goal in Case 1.

Now consider Case 2. Here, n is odd. Thus, there is one more odd integer between 0 and n than there is between 0 and $n-1$. Hence,

$$\begin{aligned}
&(\#\text{ of odd integers between 0 and } n) \\
&= (\#\text{ of odd integers between 0 and } n-1) + 1 \\
&= \left\lfloor \frac{n}{2} \right\rfloor + 1 \qquad (\text{by the IH}) \\
&= \left\lfloor \frac{n+1}{2} \right\rfloor \qquad (\text{since } n \text{ is odd}).
\end{aligned}$$

This proves the goal in Case 2.

So the goal is proved in both cases, and the induction step is complete. □

This proof was called "informal" because we don't have a formal definition of the size of a set (i.e., of what "the number of something" means). Once we have such a definition, it will become a rigorous proof.

Incidentally, let me state an even simpler formula, which however is very important:

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 precisely $b-a+1$ integers between a and b (inclusive).

Proof. Easy induction on b. □

The hard part about this proposition is to remember the "+1". It comes from our choice of including both a and b.

Convention 4.2.3. The symbol "#" means "number".

4.3. Counting subsets

4.3.1. Counting them all

Now, let us count something less trivial than numbers.

How many subsets does the set $\{1,2,3\}$ have? These subsets are

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

(Note that every set A contains both A and $\{\}$ as subsets.) So we have found 8 subsets of $\{1,2,3\}$. Are there more? No.

Likewise,

- the set $\{1,2\}$ has 4 subsets, namely $\{\}$, $\{1\}$, $\{2\}$, $\{1,2\}$;
- the set $\{1\}$ has 2 subsets, namely $\{\}$ and $\{1\}$;
- the set $\{\}$ has 1 subset, namely $\{\}$;
- the set $\{1,2,3,4\}$ has 16 subsets.

The pattern here is hard to miss:

Theorem 4.3.1. Let $n \in \mathbb{N}$. Then,

$$(\#\text{ of subsets of } \{1,2,\ldots,n\}) = 2^n.$$

Informal proof. We induct on n.

Base case: For $n = 0$, the theorem says that $(\#\text{ of subsets of } \{\}) = 2^0$, which is just saying that $1 = 1$.

Induction step: We proceed from $n-1$ to n. Thus, let n be a positive integer. We assume (as IH) that the theorem holds for $n-1$ instead of n, and we set out to prove it for n.

So our IH says that

$$(\#\text{ of subsets of } \{1,2,\ldots,n-1\}) = 2^{n-1}.$$

Our goal is to show that

$$(\#\text{ of subsets of } \{1,2,\ldots,n\}) = 2^n.$$

We define

- a **red set** to be a subset of $\{1,2,\ldots,n\}$ that contains n;
- a **green set** to be a subset of $\{1,2,\ldots,n\}$ that does not contain n.

For instance, for $n = 3$, the sets $\{3\}$, $\{1,3\}$, $\{2,3\}$, $\{1,2,3\}$ are red, while the sets $\varnothing$, $\{1\}$, $\{2\}$, $\{1,2\}$ are green.

Each subset of $\{1,2,\ldots,n\}$ is either red or green, but not both. Hence,

$$\begin{aligned}&(\#\text{ of subsets of } \{1,2,\ldots,n\})\\ &= (\#\text{ of red sets}) + (\#\text{ of green sets}).\end{aligned}$$

Thus it remains to count the red sets and the green sets.

Let's count the green sets first: The green sets are just the subsets of $\{1,2,\ldots,n-1\}$. By the IH, there are 2^{n-1} of them. So

$$(\#\text{ of green sets}) = 2^{n-1}.$$

Now to the red sets: I claim that they are just the green sets with an extra n inserted into them. In more detail: 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, each red set is uniquely paired with a green set and vice versa. For example, for $n = 3$, this looks as follows:

$$\begin{array}{cccccc}\text{green} & \{\} & \{1\} & \{2\} & \{1,2\}\\ \text{red} & \{3\} & \{1,3\} & \{2,3\} & \{1,2,3\}\end{array}.$$

Thus, there are equally many green sets as there are red sets. In other words,

$$(\#\text{ of red sets}) = (\#\text{ of green sets}) = 2^{n-1}.$$

Now,

$$\begin{aligned}&(\#\text{ of subsets of } \{1,2,\ldots,n\})\\ &= \underbrace{(\#\text{ of red sets})}_{=2^{n-1}} + \underbrace{(\#\text{ of green sets})}_{=2^{n-1}}\\ &= 2^{n-1} + 2^{n-1} = 2\cdot 2^{n-1} = 2^n.\end{aligned}$$

This proves the goal. So the induction is complete. □

More generally, we don't have to only look at sets of the form $\{1,2,\ldots,n\}$; we have:

Theorem 4.3.2. Let $n \in \mathbb{N}$. Let S be any n-element set. Then,

$$(\#\text{ of subsets of } S) = 2^n.$$

Informal proof. Rename the n elements of S as $1,2,\ldots,n$. Then, apply the preceding theorem. □

For example,

$$(\#\text{ of subsets of } \{\text{cat, dog, rat}\}) = 2^3 = 8.$$

4.3.2. Counting the subsets of a given size

Let us now refine our question, asking not for the # of all subsets of $\{1,2,\ldots,n\}$, but only of those with a given size k. Here, the **size** of a set means its # of elements, i.e., how many distinct elements it contains. For example, the size of the set $\left\{x^2\%5 \mid x \in \mathbb{N}\right\}$ is 3, since its only elements are 0, 1 and 4.

We denote the size of a set A by $|A|$.

Let us do an example: How many 2-element subsets does the set $\{1,2,3,4\}$ have? Here are they:

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

So their # is 6.

More generally, we can ask for the # of k-element subsets of a given n-element set. The answer turns out to be the binomial coefficient $\binom{n}{k}$. Let us state this as a theorem:

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

$$P(n) := \left(\begin{array}{c} \text{“for any number } k \text{ and any } n\text{-element set } S, \\ \text{we have } (\#\text{ of } k\text{-element subsets of } S) = \binom{n}{k}\text{”} \end{array} \right)$$

for each $n \in \mathbb{N}$.

Base case: We must prove $P(0)$. Let k be any number, and let S be any 0-element set. Thus, $S = \varnothing$. So S has only one subset, which is $\varnothing$ itself, and it is a 0-element subset. Thus,

$$(\#\text{ of } k\text{-element subsets of } S) = \begin{cases} 1, & \text{if } k = 0; \\ 0, & \text{else} \end{cases} = \binom{0}{k}.$$

So $P(0)$ is proved.

Induction step: Let n be a positive integer. Assume (as the IH) that $P(n-1)$ holds. We must prove that $P(n)$ holds.

So we consider any number k and any n-element set S. We must prove that

$$(\#\text{ of } k\text{-element subsets of } S) \stackrel{?}{=} \binom{n}{k}.$$

We rename the n elements of S as $1, 2, \ldots, n$. So we must prove that

$$(\#\text{ of } k\text{-element subsets of } \{1, 2, \ldots, n\}) \stackrel{?}{=} \binom{n}{k}.$$

To prove this, we define

- a **red set** to be a k-element subset of $\{1, 2, \ldots, n\}$ that contains n;
- a **green set** to be a k-element subset of $\{1, 2, \ldots, n\}$ that does not contain n.

For instance, for $n = 5$ and $k = 2$, the red sets are

$$\{1,5\},\ \{2,5\},\ \{3,5\},\ \{4,5\},$$

whereas the green sets are

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

Each k-element subset of $\{1, 2, \ldots, n\}$ is either red or green. Hence,

$$\begin{aligned}&(\#\text{ of } k\text{-element subsets of } \{1, 2, \ldots, n\})\\ &= (\#\text{ of red sets}) + (\#\text{ of green sets}).\end{aligned}$$

The green sets are just the k-element subsets of $\{1, 2, \ldots, n-1\}$. So by the IH, we have

$$(\#\text{ of green sets}) = \binom{n-1}{k}$$

(since $\{1, 2, \ldots, n-1\}$ is an $(n-1)$-element set).

Now to the red sets. If T is a red set, then $T \setminus \{n\}$ is a $(k-1)$-element subset of $\{1, 2, \ldots, n-1\}$. Conversely, if U is a $(k-1)$-element subset of $\{1, 2, \ldots, n-1\}$, then $U \cup \{n\}$ is a red set. This sets up a one-to-one correspondence between the red sets and the $(k-1)$-element subsets of $\{1, 2, \ldots, n-1\}$. As a result,

$$\begin{aligned}&(\#\text{ of red sets})\\ &= (\#\text{ of } (k-1)\text{-element subsets of } \{1, 2, \ldots, n-1\})\\ &= \binom{n-1}{k-1} \qquad (\text{by the IH}).\end{aligned}$$

Combining what we have shown, we get

$$\begin{aligned}&(\#\text{ of } k\text{-element subsets of } \{1, 2, \ldots, n\})\\ &= \underbrace{(\#\text{ of red sets})}_{=\binom{n-1}{k-1}} + \underbrace{(\#\text{ of green sets})}_{=\binom{n-1}{k}}\\ &= \binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k} \qquad (\text{by Pascal's recurrence}).\end{aligned}$$

This proves $P(n)$ and thus completes our 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 is delimited using parentheses: i.e., the list that contains the objects $a_1, a_2, \ldots, a_n$ is written $(a_1, a_2, \ldots, a_n)$.

"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 $n = m$, and
- we have $a_i = b_i$ for each $i \in \{1, 2, \ldots, n\}$.

For example:

- The lists $(1, 2)$ and $(2, 1)$ are not equal, though $\{1, 2\} = \{2, 1\}$.
- The lists $(1, 2)$ and $(1, 1, 2)$ are not equal, though $\{1, 2\} = \{1, 1, 2\}$.
- The lists $(1, 1, 2)$ and $(1, 2, 2)$ are not equal, though $\{1, 1, 2\} = \{1, 2, 2\}$.

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 **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 (even though it has only 3 **distinct** entries), thus a quadruple or a 4-tuple. Meanwhile, $(5, 8)$ is a pair, i.e., a 2-tuple.

There is exactly one 0-tuple: the empty list $()$.

There are many 1-tuples: For any object o, we can form the 1-tuple (o).

4.4.2. Counting pairs

Now let us start counting lists. We begin with pairs:

- How many pairs (a, b) are there with $a, b \in \{1, 2, 3\}$? There are nine:

$$\begin{array}{lll} (1,1), & (1,2), & (1,3), \\ (2,1), & (2,2), & (2,3), \\ (3,1), & (3,2), & (3,3). \end{array}$$

Here I have laid them out in a rectangular table with 3 rows and 3 columns, where the row determines the first entry of the pair, while the column determines the second entry. Thus, their total # is $3 \cdot 3 = 9$.

- How many pairs (a,b) are there with $a,b \in \{1,2,3\}$ and $a < b$? There are three:
$$(1,2)\,, \qquad (1,3)\,, \qquad (2,3)\,.$$
- How many pairs (a,b) are there with $a,b \in \{1,2,3\}$ and $a = b$? Three again:
$$(1,1)\,, \qquad (2,2)\,, \qquad (3,3)\,.$$
- How many pairs (a,b) are there with $a,b \in \{1,2,3\}$ and $a > b$? Three again:
$$(2,1)\,, \qquad (3,1)\,, \qquad (3,2)\,.$$

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 (where the row determines the first entry and the column determines the second entry):
$$\begin{array}{cccc} (1,1)\,, & (1,2)\,, & \cdots\,, & (1,n)\,, \\ (2,1)\,, & (2,2)\,, & \cdots\,, & (2,n)\,, \\ \vdots & \vdots & \ddots & \vdots \\ (n,1)\,, & (n,2)\,, & \cdots\,, & (n,n)\,. \end{array}$$
So there are n^2 of them.

(b) In this table, a pair (a,b) satisfies $a < b$ if and only if it is placed above the main diagonal. So we need to count the cells above the main diagonal. In the first column, there are 0 of them; in the second, there is 1; in the third, there is 2; and so on; in the last column, there are $n-1$. So the total # is
$$0+1+2+\cdots+(n-1) = 1+2+\cdots+(n-1)\,.$$

(c) Now we are counting the cells of our table that are on the main diagonal. There is 1 such cell in each column, so there are n such cells in total.

(d) We can prove this similarly to part **(b)**.

Alternatively, we can derive this from **(b)**: The pairs (a,b) that satisfy $a > b$ are in one-to-one correspondence with the pairs (a,b) that satisfy $a < b$: Namely, each former pair becomes a latter pair if we swap its entries, and vice versa. Thus, the # of former pairs equals the # of latter pairs. But we already know that the # of latter parts is $1+2+\cdots+(n-1)$ (by part **(b)**). So the same holds for the # of former pairs. □

The proposition we just proved has a nice consequence: For any $n \in \mathbb{N}$, we have

$$\begin{aligned}
n^2 &= (\text{\# of pairs } (a,b) \text{ with } a,b \in \{1,2,\ldots,n\}) \\
&= (\text{\# of pairs } (a,b) \text{ with } a,b \in \{1,2,\ldots,n\} \text{ and } a < b) \\
&\qquad + (\text{\# of pairs } (a,b) \text{ with } a,b \in \{1,2,\ldots,n\} \text{ and } a = b) \\
&\qquad + (\text{\# of pairs } (a,b) \text{ with } a,b \in \{1,2,\ldots,n\} \text{ and } a > b) \\
&= (1+2+\cdots+(n-1)) + n + (1+2+\cdots+(n-1)) \\
&= 2\cdot(1+2+\cdots+(n-1)) + n \\
&= 2\cdot(1+2+\cdots+n) - n.
\end{aligned}$$

Solving this for $1+2+\cdots+n$, we obtain

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

This is the Little Gauss formula, which we proved long ago. Now we have proved it again using counting.

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 proposition above, there are 15 such pairs, since these pairs can be arranged in a table with 3 rows and 5 columns. □

The same reasoning can be generalized to give:

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,

$$(\#\text{ of triples } (a,b,c) \text{ with } a \in A \text{ and } b \in B \text{ and } c \in C) = nmp.$$

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

$$\begin{aligned}(\#\text{ of elements of } U) &= (\#\text{ of pairs } (a,b) \text{ with } a \in A \text{ and } b \in B) \\ &= nm \qquad (\text{by the previous theorem}).\end{aligned}$$

Now, we have re-encoded each triple (a,b,c) as a pair $((a,b),c)$ with $(a,b) \in U$ and $c \in C$. So

$$\begin{aligned}&(\#\text{ of triples } (a,b,c) \text{ with } a \in A \text{ and } b \in B \text{ and } c \in C) \\ &= (\#\text{ of pairs } ((a,b),c) \text{ with } (a,b) \in U \text{ and } c \in C) \\ &= (\#\text{ of pairs } (u,c) \text{ with } u \in U \text{ and } c \in C) \\ &= (nm)\,p\end{aligned}$$

(by the previous theorem, since U is an nm-element set, and C is a p-element set). Rewriting $(nm)\,p$ as nmp, we get precisely the claim. □

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, $\{3,4\} \times \{1,7\}$ is the set of all pairs (a,b) with $a \in \{3,4\}$ and $b \in \{1,7\}$. These pairs are

$$(3,1), \qquad (3,7), \qquad (4,1), \qquad (4,7).$$

A similar notation exists for sets of triples, quadruples or k-tuples:

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 example, the set $\{1,2\} \times \{5\} \times \{2,7,6\}$ consists of all triples (a_1, a_2, a_3) with $a_1 \in \{1,2\}$ and $a_2 \in \{5\}$ and $a_3 \in \{2,7,6\}$. These triples are

$$\begin{array}{lll} (1,5,2)\,, & (1,5,7)\,, & (1,5,6)\,, \\ (2,5,2)\,, & (2,5,7)\,, & (2,5,6)\,. \end{array}$$

The word "Cartesian" in "Cartesian product" is a reference to Cartesian coordinates. Descartes's relevant insight was that (Euclidean) space can be described as the Cartesian product $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$, meaning that each point in space corresponds uniquely to a triple (x, y, z) of real numbers (its three coordinates in a given coordinate system).

Using Cartesian products, we can rewrite our above two 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, if B is an m-element set, and if 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 given $n \in \mathbb{N}$, 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 $a < b < c$? Each such triple 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) with $a < b < c$ if we list its elements in increasing order. Thus, the triples (a, b, c) of elements of $\{1, 2, \ldots, n\}$ satisfying $a < b < c$ are just the 3-element subsets of $\{1, 2, \ldots, n\}$ in disguise (i.e., the former are in one-to-correspondence with the latter). Hence,

$$\begin{aligned} &(\#\text{ of triples } (a,b,c) \text{ of elements of } \{1,2,\ldots,n\} \text{ satisfying } a<b<c) \\ &= (\#\text{ of 3-element subsets of } \{1,2,\ldots,n\}) \\ &= \binom{n}{3} \qquad (\text{by a theorem from the previous section})\,. \end{aligned}$$

More generally, for any $k \in \mathbb{N}$, we have

$$\begin{aligned}&(\#\text{ of } k\text{-tuples } (a_1, a_2, \ldots, a_k) \text{ of elements of } \{1, 2, \ldots, n\} \text{ satisfying } a_1 < a_2 < \cdots < a_k)\\ &= \binom{n}{k} \qquad (\text{by a similar argument}).\end{aligned}$$

In comparison,

$$\begin{aligned}&(\#\text{ of } k\text{-tuples } (a_1, a_2, \ldots, a_k) \text{ of elements of } \{1, 2, \ldots, n\})\\ &= \underbrace{nn\cdots n}_{k \text{ times}} = n^k.\end{aligned}$$

Not all counting problems have answers this simple. For instance, it is not hard to show that

$$\begin{aligned}&(\#\text{ of } k\text{-tuples } (a_1, a_2, \ldots, a_k) \text{ of elements of } \{1, 2, \ldots, n\} \text{ with largest entry } a_1)\\ &= 1^{k-1} + 2^{k-1} + 3^{k-1} + \cdots + n^{k-1},\end{aligned}$$

which cannot be simplified. For fixed k, there are closed formulas:

$$\begin{aligned}1^0 + 2^0 + 3^0 + \cdots + n^0 &= \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = n;\\ 1^1 + 2^1 + 3^1 + \cdots + n^1 &= 1 + 2 + \cdots + n = \frac{n(n+1)}{2};\\ 1^2 + 2^2 + 3^2 + \cdots + n^2 &= \frac{n(n+1)(2n+1)}{6};\\ 1^3 + 2^3 + 3^3 + \cdots + n^3 &= \frac{n^2(n+1)^2}{4};\\ 1^4 + 2^4 + 3^4 + \cdots + n^4 &= \frac{n(2n+1)(n+1)\left(3n+3n^2-1\right)}{30};\\ &\ldots.\end{aligned}$$

Such a closed-form expression for $1^m + 2^m + \cdots + n^m$ exists for any fixed m (see reference in the notes), but there is no uniform formula that works for all n.

In the next two chapters, we will formalize the meaning of "counting". To do so, we first have to introduce **functions** (aka **maps**).

5. Maps (aka functions)

5.1. 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 example, the "$f(t) = t^2$" function takes a real number t and outputs its square t^2.

You can thus think of a function as a rule for producing an output from an input. This gives the following **provisional** definition of a function:

Definition 5.1.1 (Informal definition of a function)**.** Let X and Y be two sets. A **function** from X to Y is (provisionally) a rule that transforms each element of X into some element of Y.

This is kicking the can down the road: What is a "rule"? Nevertheless, this "definition" gives the right intuition for a function, as long as it is correctly understood. Let me clarify it:

- A function has to "work" for each element of X. It cannot decline to operate on some elements! Thus, "take the reciprocal" is not a function from $\mathbb{R}$ to $\mathbb{R}$, since it could not work on 0 (since 0 has no reciprocal). However, "take the reciprocal" is a function from $\mathbb{R} \setminus \{0\}$ to $\mathbb{R}$.
- A function must not be ambiguous. Each input must produce exactly one output. Thus, "take your number to some random power" is not a function from $\mathbb{R}$ to $\mathbb{R}$, since different powers give different results.
- We write "$f : X \to Y$" for "f is a function from X to Y".
- If a function is called f, then the result of applying it to a given input x is denoted by $f(x)$. (This is sometimes written fx.)
- Instead of saying "$f(x) = y$", we can say "f transforms x into y" or "f sends x to y" or "f maps x to y" or "f takes the value y at x" or "y is the value of f at x" or "y is the image of x under f" or "applying f to x yields y" or "f takes x to y" or "$f : x \mapsto y$".

  For instance, if f is the "take a square" function from $\mathbb{R}$ to $\mathbb{R}$, then $f(2) = 2^2 = 4$, so that f transforms 2 into 4, or sends 2 to 4, or takes the value 4 at 2, etc., or $f : 2 \mapsto 4$.

  Do not confuse the $\to$ and $\mapsto$ arrows: The first is for sets, while the second is for specific input/output pairs.
- 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 algorithms implemented in code, and two algorithms might be different even when they compute the same output.

  In mathematics, this is not how functions are viewed: In mathematics, only the domain (= the set of all allowed inputs), the target (= the set of

all allowed outputs) and the output values matter, not how they are computed (actually, for some functions, there might not be a way to compute the outputs).

So when are two functions considered to be equal?

Two functions $f_1 : X_1 \to Y_1$ and $f_2 : X_2 \to Y_2$ are said to be **equal** if and only if

$$\begin{array}{ccccc} X_1 = X_2 & \text{and} & Y_1 = Y_2 & \text{and} \\ f_1(x) = f_2(x) & & \text{for all } x \in X_1. & \end{array}$$

Here is an example of two equal functions:

- the function $f_1 : \mathbb{R} \to \mathbb{R}$ that sends each number x to x^2;
- the function $f_2 : \mathbb{R} \to \mathbb{R}$ that sends each number x to $|x|^2$.

- If $f : Y \to Z$ and $g : X \to Y$ are functions, then $f \circ g$ (read as "f **after** g" or "the **composition** of f and g") means the function from X to Z that applies g first and then f. In other words, it is the function from X to Z that sends each $x \in X$ to $f(g(x))$.

  For example, if $f : \mathbb{R} \to \mathbb{R}$ is the sin function, and $g : \mathbb{R} \to \mathbb{R}$ is the "take the square" function, then $f \circ g$ is the function that takes each x to $\sin\left(x^2\right)$.

  Note: In general, $f \circ g$ and $g \circ f$ are not the same! For example, if $f : \mathbb{R} \to \mathbb{R}$ is the sin function, and $g : \mathbb{R} \to \mathbb{R}$ is the "take the square" function, then $g \circ f$ is the function that takes each x to $(\sin x)^2$, which is not the same as $\sin\left(x^2\right)$.

- The notation

$$\begin{array}{l} X \to Y, \\ x \mapsto (\text{some expression involving } x) \end{array}$$

  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 $\dfrac{1}{1+x}$ or $x^3 - x^{15}$.

  For instance,

$$\begin{array}{l} \mathbb{R} \to \mathbb{R}, \\ x \mapsto x^2 \end{array}$$

  is the "take the square" function (i.e., the function from $\mathbb{R}$ to $\mathbb{R}$ that sends each element x of $\mathbb{R}$ to x^2). For another example,

$$\begin{array}{l} \mathbb{R} \to \mathbb{R}, \\ x \mapsto \dfrac{x}{\sin x + 18} \end{array}$$

is the function that takes the sine of the input, then adds 18, then divides the input by the result.

For another example,

$$\begin{aligned} \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto 2 \end{aligned}$$

is the constant function that sends each input to 2.

For yet another example,

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Q}, \\ x &\mapsto 2^x \end{aligned}$$

is the function that takes each integer x to the power of 2 that has this integer as its exponent. Here are some of its values:

$$\begin{array}{cccccc} x & -2 & -1 & 0 & 1 & 2 \\ 2^x & \frac{1}{4} & \frac{1}{2} & 1 & 2 & 4 \end{array}.$$

- The notation

$$\begin{aligned} f : X &\to Y, \\ x &\mapsto (\text{some expression involving } x) \end{aligned}$$

means that we take the function from X to Y that sends each $x \in X$ to the expression on the right hand side, and we call this function f. For example, if we write

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto x^2 + 1, \end{aligned}$$

then f henceforth will denote the function from $\mathbb{R}$ to $\mathbb{R}$ that sends each x 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, I can define a function $h : \{1, 3, 5\} \to \mathbb{N}$ by

$$\begin{aligned} h(1) &= 14, \\ h(2) &= 19, \\ h(3) &= 14. \end{aligned}$$

The values here have been chosen at whim. A function needs not be "natural" or "meaningful" in any way.

- 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, so that we can later speak of the "domain" and the "target" of a function. Namely, the **domain** of a function $f : X \to Y$ is defined to be the set X, whereas the **target** of a function $f : X \to Y$ is defined to be the set Y. Thus, the functions g_1 and g_2 have different domains (g_1 has domain $\mathbb{Z}$ but g_2 has domain $\mathbb{N}$), whereas the functions g_2 and g_3 have different targets (g_2 has target $\mathbb{Q}$ but g_3 has target $\mathbb{N}$).

At this point, we have a good idea of what a function is, but not quite a rigorous definition. This can become a problem if we want to define a function that has no simple formula and no finite list of values.

Thus, we need a more rigorous definition as a backup. This will be done soon, using the more general concept of a **relation**.

5.2. Relations

Relations (to be specific: binary relations) are another concept that you have seen on many examples:

- The relation $\subseteq$ is a relation between two sets. For example, $\{1,3\} \subseteq \{1,2,3,4\}$ but $\{1,5\} \not\subseteq \{1,2,3,4\}$.
- The order relations $\leq$ and $<$ and $>$ and $\geq$ are relations between two integers (or rational numbers, or real numbers). For example, $1 \leq 5$ but $1 \not\leq -1$.
- The containment relation $\in$ is a relation between an object and a set. For instance, $1 \in \{1,2,3\}$ but $5 \notin \{1,2,3\}$.

- The implication relation $\implies$ is a relation between two statements. For example, ($n \geq 3$ is prime) $\implies$ (n is odd) but ($n \geq 1$ is prime) $\not\implies$ (n is odd).
- The divisibility relation $\mid$ is a relation between two integers.
- The relation "coprime" is a relation between two integers.
- In plane geometry, there are lots of relations: "parallel", "perpendicular", "congruent", "similar", "directly similar", etc.
- For any given integer n, the relation "congruent modulo n" is a relation between two integers. Let me call it $\overset{n}{\equiv}$. Thus, $a \overset{n}{\equiv} b$ holds if and only if $a \equiv b \bmod n$. 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 that is either true or false. For example, the relation "coprime" applied to the pair $(5, 8)$ gives the statement "5 is coprime to 8", which is true.

Generally, a relation between two sets X and Y should be applicable to any pair (x, y) with $x \in X$ and $y \in Y$, and applying it to such a pair should give a statement (which is true or false depending on the pair). The easiest way to describe a relation is therefore to specify the pairs (x, y) on which the statement is true. Thus, we can identify the relation with the **set** of these pairs. This gives us the following rigorous definition of a relation:

Definition 5.2.1. 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 $(x, y) \in X \times Y$, 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 $\mid$ is a subset of $\mathbb{Z} \times \mathbb{Z}$, namely the subset

$$\begin{aligned} &\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \text{ divides } y\} \\ &= \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid \text{there exists } z \in \mathbb{Z} \text{ such that } y = xz\} \\ &= \{(x, xz) \mid x \in \mathbb{Z} \text{ and } z \in \mathbb{Z}\}. \end{aligned}$$

  For instance, the pairs $(2, 4)$ and $(3, 9)$ and $(4, 12)$ belong to this subset, but the pairs $(2, 3)$ and $(4, 10)$ and $(10, 5)$ do not.

- The coprimality relation ("coprime to") is a subset of $\mathbb{Z} \times \mathbb{Z}$, namely the subset

$$\begin{aligned}&\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \text{ is coprime to } y\} \\ &= \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid \gcd(x,y) = 1\}.\end{aligned}$$

  It contains $(3,8)$ and $(5,12)$ but not $(4,12)$.

- 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

$$\begin{aligned}&\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \equiv y \bmod n\} \\ &= \{(x,\ x+nz) \mid x,z \in \mathbb{Z}\}.\end{aligned}$$

- 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

$$\{(p,\ell) \in P \times L \mid \text{the point } p \text{ lies on the line } \ell\}.$$

- 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 of A satisfy $x\ E_A\ y$ if and only if they are equal.

- We can literally take any subset of $X \times Y$ (where X and Y are two sets) and it will be a relation from X to Y. For example, here is a relation from $\{1,2,3\}$ to $\{5,6,7\}$:

$$\{(1,6),\ (1,7),\ (3,5)\}.$$

  Here is 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 $1\ R\ 6$ and $1\ R\ 7$ and $3\ R\ 5$ but $1 \not R\ 5$.

Relations can be visualized by "blobs-and-arrows diagrams": To draw a relation R from a set X to a set Y, we draw both sets X and Y as "blobs", with each element of either set being a node, and we draw an arrow from the x-node to the y-node for each pair $(x,y) \in R$.

5.3. Functions, formally

We can now rigorously define what a function is:

Definition 5.3.1 (Rigorous definition of a function)**.** Let X and Y be two sets. A **function** from X to Y means a relation R from X to Y 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 is an element of X, then the unique element $y \in Y$ satisfying $x \ R \ y$ will be called $R(x)$.

For example, the equality relation E_A on a set A is a function, and so is the relation from $\{1,2,3\}$ to $\{1,2,3\}$ given by the truth table

	1	2	3
1	no	yes	no
2	yes	no	no
3	yes	no	no

,

but not all the other relations we have seen (divisbility, congruence, parallelism, subset-of, element-of).

If we denote the function

	1	2	3
1	no	yes	no
2	yes	no	no
3	yes	no	no

by f,

then $f(1) = 2$ and $f(2) = 1$ and $f(3) = 1$.

This rigorous definition of a function is equivalent to our provisional definition of a function, because

- any rule f that transforms elements of X into elements of Y becomes a relation satisfying output uniqueness by

$$R = \{(x, \ f(x)) \ \mid \ x \in X\}.$$

- Conversely, if R is a relation satisfying output uniqueness, then we obtain a rule that transforms elements of X into elements of Y, namely

$$\begin{aligned} &X \to Y, \\ &x \mapsto (\text{the unique } y \in Y \text{ such that } x \ R \ y). \end{aligned}$$

5.4. Some more examples of functions

Example 5.4.1. Consider the function

$$f_0 : \{1,2,3,4\} \to \{1,2,3,4\}$$

that sends $1,2,3,4$ to $3,2,3,3$, respectively. As a relation satisfying output uniqueness, 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 5.4.2. What about the function

$$f_1 : \{1,2,3,4\} \to \{1,2,3\},$$
$$n \mapsto n\ ?$$

I claim that such a function f_1 does not exist, since it would have to send 4 to 4, but 4 is not in the target $\{1,2,3\}$. Be careful when defining functions: The output values must actually belong to the target.

Example 5.4.3. Consider the function

$$f_2 : \{1,2,3,\ldots\} \to \{1,2,3,\ldots\},$$
$$n \mapsto (\text{the number of positive divisors of } n).$$

For example, $f_2(1) = 1$ and $f_2(2) = 2$ and $f_2(3) = 2$ and $f_2(4) = 3$. As a relation, f_2 is

$$\{(1,1),\ (2,2),\ (3,2),\ (4,3),\ (5,2),\ (6,4),\ (7,2),\ (8,4),\ \ldots\}.$$

Example 5.4.4. What about the function

$$\widetilde{f_2} : \mathbb{Z} \to \{1,2,3,\ldots\},$$
$$n \mapsto (\text{the number of positive divisors of } n)\ ?$$

There is no such $\widetilde{f_2}$, since 0 has infinitely many positive divisors, so their number is either undefined or ∞ (which is not in $\{1,2,3,\ldots\}$).

Example 5.4.5. What about the function

$$f_3 : \{1,2,3,\ldots\} \to \{1,2,3,\ldots\},$$
$$n \mapsto (\text{the smallest prime divisor of } n)\ ?$$

Again, there is no such function f_3, since $f_3(1)$ makes no sense (1 has no prime divisors).

We can fix this by declaring f_3 to be a relation, not a function. This relation simply does not have an output at 1. We can also fix this by restricting the inputs to $\{2,3,4,\ldots\}$. We get an actual function

$$\begin{aligned}\widetilde{f_3} : \{2,3,4,\ldots\} &\to \{1,2,3,\ldots\}, \\ n &\mapsto (\text{the smallest prime divisor of } n).\end{aligned}$$

Example 5.4.6. What about the function

$$\begin{aligned}f_4 : \mathbb{Q} &\to \mathbb{Z}, \\ \frac{a}{b} &\mapsto a \ ?\end{aligned}$$

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.

Again, there is no such function. Indeed, the above rule would force $f_4\left(\frac{1}{2}\right)$ to be 1 and force $f_4\left(\frac{2}{4}\right)$ to be 2. But $\frac{1}{2} = \frac{2}{4}$ and therefore $f_4\left(\frac{1}{2}\right) = f_4\left(\frac{2}{4}\right)$, a contradiction. Thus, the above rule defines a relation, but the relation does not satisfy output uniqueness.

5.5. Well-definedness

The issues that we have seen in the last few examples (supposed functions failing to exist either because their outputs make no sense, or because these outputs don't lie in Y, or because these outputs are ambiguous) are known as **well-definedness** issues. Mathematicians usually say that "a function is well-defined" when they mean that its definition does not suffer from such issues. For example, the function

$$\begin{aligned}f_4 : \mathbb{Q} &\to \mathbb{Z}, \\ \frac{a}{b} &\mapsto a\end{aligned}$$

is not well-defined (i.e., there is no such function), but the function

$$\begin{aligned}f_4 : \mathbb{Q} &\to \mathbb{Q}, \\ \frac{a}{b} &\mapsto \frac{a^2}{b^2}\end{aligned}$$

is well-defined (you can also describe it as $x \mapsto x^2$, and then it is clear that the output is unambiguous). The function

$$\begin{aligned} f_1 : \{1,2,3,4\} &\to \{1,2,3\}, \\ n &\mapsto n \end{aligned}$$

is not well-defined (since $f_1(4)$ fails to lie in the target), but the function

$$\begin{aligned} f_6 : \{1,2,3,4\} &\to \{1,2,3\}, \\ n &\mapsto 1 + (n\%3) \end{aligned}$$

is well-defined (its outputs are $2, 3, 1, 2$).

Formally speaking, there is no such thing as a non-well-defined function.

5.6. The identity function

Definition 5.6.1. For any set A, there is an **identity function** $\mathrm{id}_A : A \to A$. This is the function that sends each element $a \in A$ to a itself. In other words, it is precisely the relation E_A defined above.

In terms of blobs and arrows, it is easiest to visualize id_A by drawing corresponding nodes horizontally aligned. Then, all the arrows are horizontal.

5.7. More examples

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,

$$\begin{aligned} f : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}, \\ (a,b) &\mapsto a + b \end{aligned}$$

(which sends every pair (a,b) of integers to their sum $a+b$) is a multivariate function. Its input is a pair of integers, i.e., it really has two inputs (a and b). As a relation, it is the subset

$$\begin{aligned} &\{((a,b),\ a+b) \mid a,b \in \mathbb{Z}\} \\ &= \{((a,b),c) \mid a,b,c \in \mathbb{Z} \text{ such that } c = a+b\} \end{aligned}$$

of $(\mathbb{Z} \times \mathbb{Z}) \times \mathbb{Z}$. Of course, this function has a name: addition of integers.

Other multivariate functions are

$$\begin{aligned} f : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}, \\ (a, b) &\mapsto a - b \end{aligned}$$

(subtraction of integers) and

$$\begin{aligned} f : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}, \\ (a, b) &\mapsto ab \end{aligned}$$

(multiplication of integers), and many similar functions for other sets of numbers. Keep in mind that there is no "division" function

$$\begin{aligned} f : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}, \\ (a, b) &\mapsto a/b, \end{aligned}$$

since this would have an output for the input $(1, 0)$ and since most existing outputs would not belong to $\mathbb{Z}$.

When f is a multivariate function whose inputs are k-tuples, we commonly write $f(a_1, a_2, \ldots, a_k)$ for $f((a_1, a_2, \ldots, a_k))$. For example, if f is addition of integers, then $f(a, b) = f((a, b)) = a + b$ for all $a, b \in \mathbb{Z}$.

5.8. Composition of functions

As we already mentioned, functions can be composed if the target of one is the domain of the other. We recall the definition:

Definition 5.8.1. Let X, Y and Z be three sets. Let $f : Y \to Z$ and $g : X \to Y$ be two functions. Then, $f \circ g$ denotes the function

$$\begin{aligned} X &\to Z, \\ x &\mapsto f(g(x)). \end{aligned}$$

In other words, $f \circ g$ is the function that first applies g and then applies f. This function $f \circ g$ is called the **composition** of f with g (pronounced "f after g").

In terms of relations, if f and g are two relations F and G, then $f \circ g$ is the relation

$$\{(x, z) \mid \text{there exists } y \in Y \text{ such that } x \; G \; y \text{ and } y \; F \; z\}$$

from X to Z.

We have already seen some examples above; more can be found in the notes (§5.8). Let us state a couple basic properties of compositions:

Theorem 5.8.2 (associativity of composition)**.** Let X, Y, Z, W be four sets. Let $f : Z \to W$, $g : Y \to Z$ and $h : X \to Y$ be three functions. Then,

$$(f \circ g) \circ h = f \circ (g \circ h).$$

Proof. Argue that both sides send each $x \in X$ to the same output. See the notes for details. □

Theorem 5.8.3. Let $f : X \to Y$ be a function. Then,

$$f \circ \mathrm{id}_X = \mathrm{id}_Y \circ f = f.$$

Proof. Similar but even more trivial. □

5.9. Jectivities (injectivity, surjectivity, bijectivity)

Now we define three important properties of functions:

Theorem 5.9.1. Let $f : X \to Y$ be a function. Then:

(a) We say that f is **injective** (aka **one-to-one**, aka an **injection**) if

for each $y \in Y$, there exists **at most one** $x \in X$ such that $f(x) = y$.

In other words: f is **injective** if there are no two distinct inputs $x_1 \neq x_2$ that produce the same output (i.e., satisfy $f(x_1) = f(x_2)$).

(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 and only if f is injective and surjective.

Some examples:

- The function
$$f : \mathbb{N} \to \mathbb{N},$$
$$k \mapsto k^2$$
is injective (since no two distinct natural numbers $k, \ell \in \mathbb{N}$ have the same square $k^2 = \ell^2$) but not surjective (since not every nonnegative integer is a perfect square), and thus not bijective either.

- Let $S = \{0, 1, 4, 9, 16, 25, \ldots\}$ be the set of all perfect squares (= squares of integers). The function
$$\begin{aligned} g : \mathbb{N} &\to S, \\ k &\mapsto k^2 \end{aligned}$$
is injective (for the same reason as f) and also surjective (since each $y \in S$ is a perfect square, i.e., has the form k^2 for some $k \in \mathbb{N}$). Thus, it is bijective.

- The function
$$\begin{aligned} \widetilde{f} : \mathbb{Z} &\to \mathbb{Z}, \\ k &\mapsto k^2 \end{aligned}$$
is not injective (since $\widetilde{f}(1) = \widetilde{f}(-1)$) and not surjective either, thus definitely not bijective.

- The function
$$\begin{aligned} h : \mathbb{N} &\to \mathbb{N}, \\ k &\mapsto k//2 \end{aligned}$$
is not injective (since $h(0) = h(1)$) but surjective (since each $y \in \mathbb{N}$ is the image $h(2y)$). So it is 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 any $k \in E$) and surjective, so it is bijective.

- Let $O = \{1, 3, 5, 7, \ldots\}$ 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 any $k \in O$) and surjective, so it is bijective.

- The function
$$\begin{aligned} f : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}, \\ (a, b) &\mapsto a + b \end{aligned}$$
(this is the addition of integers) is not injective (for example, $f(0,1) = f(1,0)$) but is surjective (since $n = f(n, 0)$ for each $n \in \mathbb{Z}$).

When a function is defined on a finite set, you can list its values in a table. This makes it easy to determine whether it is in/sur/bi/nothingjective:

Remark 5.9.2. 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 in the top row (each exactly once), and the corresponding outputs $f(x)$ appears 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 the table has no two equal values.

(b) The function f is surjective if and only if each element of Y appears on the bottom row.

(c) The function f is bijective if and only if each element of Y appears exactly once on the bottom row.

For example:

- The function

$$f : \{4,6,7\} \to \{0,1,2\}, \quad k \mapsto k\%3$$

has table of values

x	4	6	7
$f(x)$	1	0	1

,

so it is not injective (since 1 appears twice in the bottom row) and not surjective (since 2 does not appear in the bottom row).

In terms of blobs-and-arrows pictures,

- a map $f : X \to Y$ is injective if and only if no two arrows hit the same Y-node;
- a map $f : X \to Y$ is surjective if and only if each Y-node is hit by at least one arrow;
- a map $f : X \to Y$ is bijective if and only if each Y-node is hit by exactly one arrow.

5.10. Inverses

5.10.1. Definition and examples

Bijective maps have a special power: they can be inverted. Here is what this means:

Definition 5.10.1. Let $f : X \to Y$ be a function. An **inverse** of f means a function $g : Y \to X$ such that

$$f \circ g = \mathrm{id}_Y \qquad \text{and} \qquad g \circ f = \mathrm{id}_X .$$

In other words, an **inverse** of f means a function $g : Y \to X$ such that

$$\begin{aligned} f(g(y)) &= y \qquad \text{for each } y \in Y, \qquad \text{and} \\ g(f(x)) &= x \qquad \text{for each } x \in X. \end{aligned}$$

Roughly speaking, an inverse of f thus means a map that both undoes and is undone by f.

Not every function has an inverse. We shall soon see which ones do. First, some examples:

- Let $f : \{1,2,3\} \to \{6,7,8\}$ be the "add 5" function (sending each x to $x+5$). Let $g : \{6,7,8\} \to \{1,2,3\}$ be the "subtract 5" function (sending each y to $y-5$). Then, g is an inverse of f, since each $y \in \{6,7,8\}$ satisfies

$$f(g(y)) = \underbrace{g(y)}_{=y-5} + 5 = y - 5 + 5 = y$$

  and similarly each $x \in \{1,2,3\}$ satisfy $g(f(x)) = x$.

- Now let f be the map

$$\begin{aligned} f : \{1,2,3,4,5\} &\to \{1,2,3,4,5\}, \\ 1 &\mapsto 3, \\ 2 &\mapsto 5, \\ 3 &\mapsto 1, \\ 4 &\mapsto 2, \\ 5 &\mapsto 4. \end{aligned}$$

This map f has an inverse – namely, the map

$$\begin{aligned} g : \{1,2,3,4,5\} &\to \{1,2,3,4,5\}, \\ 3 &\mapsto 1, \\ 5 &\mapsto 2, \\ 1 &\mapsto 3, \\ 2 &\mapsto 4, \\ 4 &\mapsto 5. \end{aligned}$$

- Let

$$\begin{aligned} f : \{1,2,3\} &\to \{1,2\}, \\ 1 &\mapsto 1, \\ 2 &\mapsto 2, \\ 3 &\mapsto 1. \end{aligned}$$

This map f has no inverse, since any inverse g of f would have to satisfy both $g(1) = 1$ and $g(1) = 3$, a contradiction. The underlying issue here is that f is not injective (specifically, $f(1) = f(3)$).

- Let

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N}, \\ i &\mapsto i + 1. \end{aligned}$$

This map f has no inverse, since any inverse g of f would have to satisfy $f(g(0)) = 0$, but 0 is not a value of f. The underlying issue here is that f is not surjective (specifically, 0 is not a value).

5.10.2. Invertibility is bijectivity

The last two examples show that in order to have an inverse, a map needs to be both injective and surjective, i.e., bijective. The converse is also true: Any bijective map has an inverse. Let us state this as a theorem:

Theorem 5.10.2. Let $f : X \to Y$ be a map between two sets X and Y. Then, f has an inverse if and only if f is bijective.

Proof. Essentially, this is clear from looking at the blobs-and-arrows picture: If f is bijective, then an inverse of f can simply be defined as the map $g : Y \to X$ that sends each $y \in Y$ to the unique $x \in X$ that satisfies $f(x) = y$. Showing that this map g really is an inverse of f is an easy exercise in manipulating equations. (See the notes.) □

So bijective maps are the same as invertible maps (= maps that have inverses).

5.10.3. Uniqueness of the inverse

Theorem 5.10.3. Let $f : X \to Y$ be a function. Then, f has at most one inverse.

Proof. We must prove that any two inverses of f are equal.

So let g_1 and g_2 be two inverses of f. We must prove that $g_1 = g_2$.

Since g_1 is an inverse of f, we have $g_1 \circ f = \mathrm{id}_X$ and $f \circ g_1 = \mathrm{id}_Y$.

Since g_2 is an inverse of f, we have $g_2 \circ f = \mathrm{id}_X$ and $f \circ g_2 = \mathrm{id}_Y$.

Now,

$$g_1 \circ \underbrace{f \circ g_2}_{=\mathrm{id}_Y} = g_1 \circ \mathrm{id}_Y = g_1,$$

so that

$$g_1 = \underbrace{g_1 \circ f}_{=\mathrm{id}_X} \circ g_2 = \mathrm{id}_X \circ g_2 = g_2,$$

as desired. □

Definition 5.10.4. Let $f : X \to Y$ be a map that has an inverse. Then, this inverse is unique (by the theorem we just proved), and thus will be called **the inverse** of f. We will denote it by f^{-1}.

So

$$f^{-1} \circ f = \mathrm{id}_X \qquad \text{and} \qquad f \circ f^{-1} = \mathrm{id}_Y .$$

That is,

$$f^{-1}(f(x)) = x \qquad \text{for each } x \in X;$$
$$f\left(f^{-1}(y)\right) = y \qquad \text{for each } y \in Y.$$

5.10.4. More examples

- Recall the bijective function

$$f : E \to \mathbb{N},$$
$$k \mapsto k//2 = k/2,$$

where $E = \{0, 2, 4, 6, \ldots\}$. Then, f has an inverse, namely

$$g : \mathbb{N} \to E,$$
$$k \mapsto 2k.$$

- Let $\mathbb{R}_{\geq 0}$ be the set of all nonnegative real numbers. Then, the function

$$f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0},$$
$$x \mapsto x^2$$

has an inverse, namely

$$\begin{aligned} g : \mathbb{R}_{\geq 0} &\to \mathbb{R}_{\geq 0}, \\ x &\mapsto \sqrt{x}. \end{aligned}$$

- The function

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto x^2 \end{aligned}$$

has no inverse, since it is not bijective.

- The function

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto x^3 \end{aligned}$$

has an inverse, called

$$\begin{aligned} g : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto \sqrt[3]{x}. \end{aligned}$$

5.10.5. Inverses of inverses and compositions

The following basic facts are easy to prove (see the notes for the proofs):

Proposition 5.10.5. Let X be any set. Then, the identity map $\mathrm{id}_X : X \to X$ is bijective, and is its own inverse.

Theorem 5.10.6. Let $f : X \to Y$ be a map that has an inverse $f^{-1} : Y \to X$. Then, f^{-1} has an inverse, namely f.

Theorem 5.10.7 (socks-and-shoes formula)**.** Let X, Y, Z be three sets. Let $f : Y \to Z$ and $g : X \to Y$ be two bijective maps. Then, the composition $f \circ g : X \to Z$ is also bijective, and its inverse is

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}.$$

Note that $g^{-1} \circ f^{-1}$ is not the same as $f^{-1} \circ g^{-1}$ (in fact, the latter might not exist).

In particular, the socks-and-shoes formula shows that a composition of two bijective maps is itself bijective. (However, sometimes a composition of non-bijective maps can also be bijective.)

See the notes for several solved exercises on in/sur/bijections and inverses.

5.11. Isomorphic sets

Definition 5.11.1. Let X and Y be two sets. We say that these 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 is symmetric: If X and Y are isomorphic, then so are Y and X (since bijective maps $f : X \to Y$ have bijective inverses $f^{-1} : Y \to X$).

Some examples:

- The sets $\{1,2,3\}$ and $\{6,7,8\}$ are isomorphic, since the "add 5" map from $\{1,2,3\}$ to $\{6,7,8\}$ is bijective.
- The sets $\{1,2,3\}$ and $\{1,2\}$ are not isomorphic, since there is no injective (let alone bijective) map from $\{1,2,3\}$ to $\{1,2\}$.
- The sets $\{1,2,3\}$ and $\{1,6,25\}$ are isomorphic, since the map sending 1 to 1, sending 2 to 6 and sending 3 to 25 is bijective.
- The sets $\mathbb{N}$ and $E := \{\text{all even nonnegative integers}\}$ are isomorphic, since the map
$$\begin{aligned} \mathbb{N} &\to E, \\ n &\mapsto 2n \end{aligned}$$
is bijective.
- The sets $\mathbb{N}$ and $O := \{\text{all odd nonnegative integers}\}$ are isomorphic, since the map
$$\begin{aligned} \mathbb{N} &\to O, \\ n &\mapsto 2n+1 \end{aligned}$$
is bijective.
- The sets $\mathbb{N}$ and $\mathbb{Z}$ are isomorphic, since there is a bijection from $\mathbb{N}$ to $\mathbb{Z}$ that sends
$$\begin{aligned} &0,1,2,3,4,5,6,7,\ldots && \text{to} \\ &0,1,-1,2,-2,3,-3,4,-4,\ldots, && \text{respectively.} \end{aligned}$$
Explicitly, this map 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

$$0,1,2,3,4,5,6,7,\ldots \qquad \text{to}$$
$$\underbrace{\frac{-1}{1}, \frac{0}{1}, \frac{1}{1}}_{\substack{\text{all reduced fractions whose numerator and denominator are } \leq 1 \text{ in absolute value (ordered from smallest to largest)}}} , \quad \underbrace{\frac{-2}{1}, \frac{-1}{2}, \frac{1}{2}, \frac{2}{1}}_{\substack{\text{all reduced fractions whose numerator and denominator are } \leq 2 \text{ in absolute value (ordered from smallest to largest)}}} , \quad \underbrace{\frac{-3}{1}, \frac{-3}{2}, \frac{-2}{3}, \frac{-1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{3}{2}, \frac{3}{1}}_{\substack{\text{all reduced fractions whose numerator and denominator are } \leq 3 \text{ in absolute value (ordered from smallest to largest)}}}, \ \ldots,$$

  respectively.

- 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

$$0,1,2,3,4,5,6,\ldots \text{ to}$$
$$\underbrace{(0,0)}_{\substack{\text{all pairs whose entries sum to } 0}} , \underbrace{(0,1), (1,0)}_{\substack{\text{all pairs whose entries sum to } 1}}, \underbrace{(0,2), (1,1), (2,0)}_{\substack{\text{all pairs whose entries sum to } 2}}, \ \ldots$$

  respectively. The inverse $f^{-1} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ of this map f can be described explicitly by

$$f^{-1}(n,m) = \frac{(n+m)(n+m+1)}{2} + n \qquad \text{for every } (n,m) \in \mathbb{N}$$

  (puzzle: why?).

- The sets $\mathbb{N}$ and $\mathbb{R}$ are **not** isomorphic, i.e., there is no bijection from $\mathbb{N}$ to $\mathbb{R}$. Proofs can be found in various textbooks; see the notes for a couple references.

6. Enumeration revisited

6.1. Counting, formally

6.1.1. Definition

As you might have noticed, isomorphic sets (i.e., sets that have a bijection going between them) have the same size – i.e., the same # of elements (at least when they are finite). We shall now use this idea to **define** the size of a set!

First, some notations:

Definition 6.1.1. **(a)** If $n \in \mathbb{N}$, then $[n]$ will denote the set $\{1, 2, \ldots, n\}$.
(b) If $a, b \in \mathbb{Z}$, then $[a, b]$ shall mean the set

$$\begin{aligned}\{a, a+1, a+2, \ldots, b\} &= \{\text{all integers } x \text{ such that } a \leq x \leq b\} \\ &= \{x \in \mathbb{Z} \mid a \leq x \leq b\}.\end{aligned}$$

If $a > b$, then this is the empty set.

For example,

$$\begin{aligned}[4] &= \{1, 2, 3, 4\}, & [1] &= \{1\}, & [0] &= \varnothing, \\ [2, 5] &= \{2, 3, 4, 5\}, & [5, 2] &= \varnothing.\end{aligned}$$

Now, we can define the size of a finite set:

Definition 6.1.2. Let $n \in \mathbb{N}$. A set S is said to have **size** n if S is isomorphic to $[n]$ (that is, if there is a bijection from S to $[n]$).

For instance:

- The set $\{4, 6, 8, 10\}$ has size 4, since the map

$$\begin{aligned}\{4, 6, 8, 10\} &\to [4], \\ 4 &\mapsto 1, \\ 6 &\mapsto 2, \\ 8 &\mapsto 3, \\ 10 &\mapsto 4\end{aligned}$$

  is a bijection.

- The set $\mathbb{N}$ is infinite, so there is no bijection from $\mathbb{N}$ to $[n]$ 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 6.1.3. 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 some $s \in S$ such that $S \setminus \{s\}$ has size $n - 1$.

This recursive definition reduces the question of "what is a set of size n" to the simpler question "what is a set of size $n - 1$", which (by induction) makes it possible to answer the question.

Theorem 6.1.4. (a) The above two definitions of size are equivalent.
(b) The size of a finite set is determined uniquely – i.e., a set cannot have two different sizes at the same time.

We will not prove this here.

Definition 6.1.5. (a) An **n-element set** (for some $n \in \mathbb{N}$) means a set of size n.
(b) A set is said to be **finite** if it has size n for some $n \in \mathbb{N}$.
(c) 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, the # of odd integers between 2 and 8 is the size of the set $\{\text{odd integers between 2 and 8}\}$. This size is 3. Also, $|\{4,6,8,10\}| = 4$. Also, $|\{5,6,5\}| = 2$.

6.1.2. Rules for sizes of finite sets

The following rules (some of which we have already encountered in other words) are common sense, but very useful in counting.

Theorem 6.1.6 (Bijection Principle)**.** Let A and B be two finite sets. Then, $|A| = |B|$ if and only if there exists a bijection from A to B.

Theorem 6.1.7. For each $n \in \mathbb{N}$, we have $|[n]| = n$.

Theorem 6.1.8. Let S be a set. Then:
(a) We have $|S| = 0$ if and only if S 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 6.1.9. Let S be a finite set. Let t be an object such that $t \notin S$. Then,

$$|S \cup \{t\}| = |S| + 1.$$

Theorem 6.1.10 (Sum rule for two sets)**.** Let A and B be two disjoint finite sets. Then, the set $A \cup B$ is again finite, and its size is

$$|A \cup B| = |A| + |B|.$$

Theorem 6.1.11 (Sum rule for k sets)**.** Let $A_1, A_2, \ldots, A_k$ be k disjoint finite sets. Then, the set $A_1 \cup A_2 \cup \cdots \cup A_k$, and its size is

$$|A_1 \cup A_2 \cup \cdots \cup A_k| = |A_1| + |A_2| + \cdots + |A_k|.$$

Theorem 6.1.12 (Difference rule)**.** Let T be a subset of a finite set S. Then:
(a) The set T is finite, and its size satisfies $|T| \leq |S|$.
(b) We have $|S \setminus T| = |S| - |T|$.
(c) If $|T| = |S|$, then $T = S$.

Theorem 6.1.13 (Product rule for two sets)**.** Let A and B be 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 6.1.14 (Product rule for k sets)**.** Let $A_1, A_2, \ldots, A_k$ be any k finite sets. Then, the set

$$\begin{aligned} &A_1 \times A_2 \times \cdots \times A_k \\ &= \{\text{all } k\text{-tuples } (a_1, a_2, \ldots, a_k) \text{ with } a_i \in A_i \text{ for each } i \in [k]\} \end{aligned}$$

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 are the basic counting rules. There are a few more which can be derived from them. For example:

Theorem 6.1.15. Let A and B be two finite sets (not necessarily disjoint). Then,

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Theorem 6.1.16. Let A, B, C be three finite sets. Then,

$$\begin{aligned} &|A \cup B \cup C| \\ &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|. \end{aligned}$$

These two theorems are the start of a pattern known as the "principle of inclusion and exclusion" aka "Sylvester's sieve formula".

6.2. Redoing some proofs rigorously

We have previously proved some counting theorems somewhat informally. Let us now revisit those proofs briefly and see how to formalize them. (See the notes for much more detail.)

Proposition 6.2.1. 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).

Proof. As we said, this can be proved by induction on b, but let us give a different proof now:

Consider the map

$$f : \underbrace{[b-a+1]}_{\substack{=[1,b-a+1] \\ =\{1,2,\ldots,b-a+1\}}} \to \underbrace{[a,b]}_{=\{a,a+1,\ldots,b\}}, \qquad i \mapsto i+(a-1).$$

This map f just adds $a-1$ to its input. This map f has an inverse: namely, the map

$$g : \underbrace{[a,b]}_{=\{a,a+1,\ldots,b\}} \to \underbrace{[b-a+1]}_{\substack{=[1,b-a+1] \\ =\{1,2,\ldots,b-a+1\}}}, \qquad j \mapsto j-(a-1).$$

Proving that these maps f and g are mutually inverse is trivial. So the map f has an inverse, i.e., is a bijection. Thus, we have found a bijection from $[b-a+1]$ to $[a,b]$ (namely, f). Hence, by the bijection principle, $|[b-a+1]| = |[a,b]|$. Therefore,

$$|[a,b]| = |[b-a+1]| = b-a+1,$$

qed. □

Now, let us revisit our first theorem about counting subsets:

Theorem 6.2.2. Let $n \in \mathbb{N}$. Then,

$$(\#\text{ of subsets of } [n]) = 2^n.$$

Rigorous proof. We induct on n.

Base case: For $n=0$, the theorem says that $(\#\text{ of subsets of } [0]) = 2^0$, which is just saying that $1=1$.

Induction step: We proceed from $n-1$ to n. Thus, let n be a positive integer. We assume (as IH) that the theorem holds for $n-1$ instead of n, and we set out to prove it for n.

So our IH says that

$$(\#\text{ of subsets of } [n-1]) = 2^{n-1}.$$

Our goal is to show that

$$(\#\text{ of subsets of } [n]) = 2^n.$$

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 instance, for $n = 3$, the sets $\{3\}$, $\{1,3\}$, $\{2,3\}$, $\{1,2,3\}$ are red, while the sets $\varnothing$, $\{1\}$, $\{2\}$, $\{1,2\}$ are green.

Each subset of $[n]$ is either red or green, but not both. Hence,

$$\{\text{subsets of } [n]\} = \{\text{red sets}\} \cup \{\text{green sets}\},$$

and the two sets $\{\text{red sets}\}$ and $\{\text{green sets}\}$ are disjoint. Therefore, by the sum rule,

$$|\{\text{red sets}\} \cup \{\text{green sets}\}| = |\{\text{red sets}\}| + |\{\text{green sets}\}|.$$

In other words,

$$|\{\text{subsets of } [n]\}| = |\{\text{red sets}\}| + |\{\text{green sets}\}|.$$

In other words,

$$(\#\text{ of subsets of } [n]) = (\#\text{ of red sets}) + (\#\text{ of green sets}).$$

Thus it remains to count the red sets and the green sets.

Let's count the green sets first: The green sets are just the subsets of $[n-1]$. By the IH, there are 2^{n-1} of them. So

$$(\#\text{ of green sets}) = 2^{n-1}.$$

Now to the red sets: I claim that they are just the green sets with an extra n inserted into them. In more detail: 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 means that we can define two maps

$$\begin{aligned} \text{ins}_n : \{\text{green sets}\} &\to \{\text{red sets}\}, \\ G &\mapsto G \cup \{n\} \end{aligned}$$

and

$$\begin{aligned} \text{rem}_n : \{\text{red sets}\} &\to \{\text{green sets}\}, \\ R &\mapsto R \setminus \{n\}, \end{aligned}$$

and these two maps are mutually inverse, so they are bijections. Therefore, by the bijection principle,

$$\begin{aligned} |\{\text{red sets}\}| &= |\{\text{green sets}\}|, \qquad \text{i.e.} \\ (\#\text{ of red sets}) &= (\#\text{ of green sets}). \end{aligned}$$

Thus,

$$(\#\text{ of red sets}) = (\#\text{ of green sets}) = 2^{n-1}.$$

Now,

$$\begin{aligned} &(\#\text{ of subsets of } [n]) \\ &= \underbrace{(\#\text{ of red sets})}_{=2^{n-1}} + \underbrace{(\#\text{ of green sets})}_{=2^{n-1}} \\ &= 2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n. \end{aligned}$$

This proves the goal. So the induction is complete. □

More generally, we don't have to only look at sets of the form $[n]$; we have:

Theorem 6.2.3. Let $n \in \mathbb{N}$. Let S be any n-element set. Then,

$$(\#\text{ of subsets of } S) = 2^n.$$

Rigorous proof. Since S has size n, there exists a bijection $\alpha : S \to [n]$. Pick such an α. As a bijection, α has an inverse α^{-1}.

Now, let us "extend" this bijection α to the subsets of S (rather than the elements of S). Namely, we define a map

$$\begin{aligned} \alpha_* : \{\text{subsets of } S\} &\to \{\text{subsets of } [n]\}, \\ T &\mapsto \{\alpha(t) \mid t \in T\}, \\ \text{equivalently } \{s_1, s_2, \ldots, s_k\} &\mapsto \{\alpha(s_1), \alpha(s_2), \ldots, \alpha(s_k)\}. \end{aligned}$$

This map α_* is again a bijection, since it has an inverse $\left(\alpha^{-1}\right)_*$. Therefore, by the bijection principle,

$$|\{\text{subsets of } S\}| = |\{\text{subsets of } [n]\}|.$$

In other words,

$$(\#\text{ of subsets of } S) = (\#\text{ of subsets of } [n]) = 2^n$$

by the preceding theorem. Proof complete. □

Similarly, we can formalize the proofs of the $\binom{n}{k}$ formula (for the # of k-element subsets of an n-element set) and of the other counting results we have proved before.

You don't have to do this on the MT!

Let me derive a simple corollary:

Corollary 6.2.4. Let $n \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Proof. Consider the n-element set $[n] = \{1, 2, \ldots, n\}$. This set has size n, so that each subset of $[n]$ has size ≥ 0 and $\leq n$. Thus, by the sum rule,

$$\begin{aligned}
&(\text{\# of subsets of } [n]) \\
&= (\text{\# of 0-element subsets of } [n]) \\
&\qquad + (\text{\# of 1-element subsets of } [n]) \\
&\qquad + (\text{\# of 2-element subsets of } [n]) \\
&\qquad + \cdots \\
&\qquad + (\text{\# of } n\text{-element subsets of } [n]) \\
&= \sum_{k=0}^{n} \underbrace{(\text{\# of } k\text{-element subsets of } [n])}_{= \binom{n}{k}} \\
&= \sum_{k=0}^{n} \binom{n}{k}.
\end{aligned}$$

Thus,

$$\sum_{k=0}^{n} \binom{n}{k} = (\text{\# of subsets of } [n]) = 2^n.$$

□

6.3. Lacunar subsets

Another type of objects we can count are the so-called **lacunar subsets**. Here is their definition:

Definition 6.3.1. A set S of integers is called **lacunar** if it contains no two consecutive integers (i.e., if there is no $i \in \mathbb{Z}$ such that both i and $i+1$ belong to S).

For example, the set $\{2,4,7\}$ is lacunar, but the set $\{1,2,5\}$ is not. Any 1-element set of integers is lacunar, and so is the empty set.

Now three natural questions can be asked: For a given $n \in \mathbb{N}$,

1. how many lacunar subsets does $[n]$ have?
2. how many k-element lacunar subsets does $[n]$ have for a given $k \in \mathbb{N}$?
3. what is the largest size of a lacunar subset of $[n]$?

We shall answer these three questions in the present section. First, question 3:

Proposition 6.3.2. 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. □

Now let us count the lacunar subsets. This is an easy question to experiment on in any programming language, so we can just run it for $n = 0, 1, \ldots, 9$ and see whether the results look recognizable:

n	0	1	2	3	4	5	6	7	8	9
# of lacunar subsets of $[n]$	1	2	3	5	8	13	21	34	55	89

For example, for $n = 4$, the lacunar subsets of $[4]$ are

$$\varnothing,\ \{1\},\ \{2\},\ \{3\},\ \{4\},\ \{1,3\},\ \{1,4\},\ \{2,4\}.$$

The table above reminds us of the Fibonacci numbers. And indeed, these numbers are the Fibonacci numbers f_{n+2}:

Theorem 6.3.3. For any integer $n \geq -1$, we have

$$(\#\text{ of lacunar subsets of } [n]) = f_{n+2}.$$

Here, we agree that $[-1] := \varnothing$, and more generally, $[k] := \varnothing$ for any $k \leq 0$.

Proof. Let

$$\ell_n := (\#\text{ of lacunar subsets of } [n]) \qquad \text{for any } n \geq -1.$$

So we must prove that

$$\ell_n = f_{n+2} \qquad \text{for each } n \geq -1.$$

To prove this, it sounds like a good idea to express ℓ_n in terms of ℓ_{n-1} and ℓ_{n-2}; specifically, we would hope to show that $\ell_n = \ell_{n-1} + \ell_{n-2}$ for each $n \geq 1$. If we can show this, then (assuming that we can also show $\ell_{-1} = f_1$ and $\ell_0 = f_2$) we can conclude by strong induction that $\ell_n = f_{n+2}$ for each n.

Showing that $\ell_{-1} = f_1$ and $\ell_0 = f_2$ is easy: All four values are 1. Now we need to prove that:

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

$$\begin{aligned}\ell_n &= (\#\text{ of lacunar subsets of } [n]) \\ &= (\#\text{ of red lacunar subsets of } [n]) + (\#\text{ of green lacunar subsets of } [n]).\end{aligned}$$

The green lacunar subsets of $[n]$ are just the lacunar subsets of $[n-1]$. So

$$\begin{aligned}&(\#\text{ of green lacunar subsets of } [n]) \\ &= (\#\text{ of lacunar subsets of } [n-1]) = \ell_{n-1}.\end{aligned}$$

What about the red ones? If R is a red lacunar subset of $[n]$, then $n \in R$, thus $n-1 \notin R$ (since R is lacunar), and therefore $R \setminus \{n\}$ is a lacunar subset of $[n-2]$. So we obtain a map

$$\begin{aligned}\operatorname{rem}_n : \{\text{red lacunar subsets of } [n]\} &\to \{\text{lacunar subsets of } [n-2]\}, \\ R &\mapsto R \setminus \{n\}.\end{aligned}$$

Conversely, if L is a lacunar subset of $[n-2]$, then $L \cup \{n\}$ is a red lacunar subset of $[n]$ (since the n added to L will not be adjacent to any existing element of L). Thus, we obtain a map

$$\begin{aligned}\operatorname{ins}_n : \{\text{lacunar subsets of } [n-2]\} &\to \{\text{red lacunar subsets of } [n]\}, \\ L &\mapsto L \cup \{n\}.\end{aligned}$$

It is clear that the maps rem_n and ins_n are inverses of each other. Thus, they are bijections. Hence, by the bijection principle,

$$|\{\text{red lacunar subsets of } [n]\}| = |\{\text{lacunar subsets of } [n-2]\}|.$$

In other words,

$$\begin{aligned}&(\#\text{ of red lacunar subsets of } [n])\\&= (\#\text{ of lacunar subsets of } [n-2]) = \ell_{n-2}.\end{aligned}$$

Thus, as we know,

$$\begin{aligned}\ell_n &= \underbrace{(\#\text{ of red lacunar subsets of } [n])}_{=\ell_{n-2}} + \underbrace{(\#\text{ of green lacunar subsets of } [n])}_{=\ell_{n-1}}\\&= \ell_{n-2} + \ell_{n-1} = \ell_{n-1} + \ell_{n-2}.\end{aligned}$$

This proves Claim 1. □

Now recall that our goal is to prove that $\ell_n = f_{n+2}$ for each $n \geq -1$. In other words, we must prove that the two sequences $(\ell_{-1}, \ell_0, \ell_1, \ldots)$ and $(f_1, f_2, f_3, \ldots)$ are equal. But this is now easy: These two sequences

- have the same two starting entries $\ell_{-1} = f_1$ and $\ell_0 = f_2$, and
- satisfy the same recursion ($\ell_n = \ell_{n-1} + \ell_{n-2}$ for each $n \geq 1$, and $f_n = f_{n-1} + f_{n-2}$ for each $n \geq 2$).

This entails that they are equal (by induction). □

There remains one question of the three that we posed: counting the k-element lacunar subsets of $[n]$ for given n and k. Looking at a table makes us suspect the following pattern:

Theorem 6.3.4. 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, as before using green and red sets.

Here is a nicer way, which reduces this to the combinatorial interpretation of BCs. Namely, we shall construct a bijection

$$\begin{aligned}&\text{from } \{k\text{-element lacunar subsets of } [n]\}\\&\text{to } \{k\text{-element subsets of } [n+1-k]\}.\end{aligned}$$

The idea of this bijection is to move the elements of our lacunar subset closer to each other by subtracting 0 from the smallest element, subtracting 1 from the second-smallest element, subtracting 2 from the third-smallest, and so on. To put this in formulas: If S is a k-element lacunar subset of $[n]$, and if $s_1, s_2, \ldots, s_k$

are the elements of S in increasing order, then the image of S under our bijection will be the subset

$$\{s_1 - 0,\ \ s_2 - 1,\ \ s_3 - 2,\ \ \ldots,\ \ s_k - (k-1)\} \text{ of } [n+1-k].$$

Notice that the relative order of the elements is preserved by this operation: i.e., we still have

$$s_1 - 0 < s_2 - 1 < s_3 - 2 < \cdots < s_k - (k-1),$$

since the set S was lacunar.

To prove that this map is a bijection, we construct its inverse: This inverse takes any k-element subset T of $[n+1-k]$, lists its elements as $t_1, t_2, \ldots, t_k$ in increasing order, and sends it to the lacunar subset

$$\{t_1 + 0,\ \ t_2 + 1,\ \ t_3 + 2,\ \ \ldots,\ \ t_k + (k-1)\} \text{ of } [n].$$

Thus, we have found a bijection

$$\begin{aligned} &\text{from } \{k\text{-element lacunar subsets of } [n]\} \\ &\text{to } \{k\text{-element subsets of } [n+1-k]\}. \end{aligned}$$

Hence, the bijection principle yields

$$\begin{aligned} &(\#\text{ of } k\text{-element lacunar subsets of } [n]) \\ &= (\#\text{ of } k\text{-element subsets of } [n+1-k]) = \binom{n+1-k}{k}. \end{aligned}$$

□

Note that we have tacitly used the following fundamental fact:

Proposition 6.3.5. Let $k \in \mathbb{N}$. Let S be a k-element set of integers. Then, we can list the elements of S uniquely in increasing order. In other words, there exists a unique k-tuple $(s_1, s_2, \ldots, s_k)$ of integers such that

$$\{s_1, s_2, \ldots, s_k\} = S \qquad \text{and} \qquad s_1 < s_2 < \cdots < s_k.$$

So now we have answered all three questions about lacunar subsets. We actually get two different-looking answers to Question 2: On the one hand, we have shown that

$$(\#\text{ of lacunar subsets of } [n]) = f_{n+2};$$

on the other hand, the sum rule yields

$$\begin{aligned}
&(\#\text{ of lacunar subsets of } [n]) \\
&= \sum_{k=0}^{n} \underbrace{(\#\text{ of } k\text{-element lacunar subsets of } [n])}_{= \binom{n+1-k}{k}} \\
&= \sum_{k=0}^{n} \binom{n+1-k}{k} = \binom{n+1}{0} + \binom{n}{1} + \binom{n-1}{2} + \cdots + \binom{0}{n+1}.
\end{aligned}$$

Comparing these two equalities, we obtain

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

Substituting $n-1$ for n in this equality, we transform it into the following nicer form:

Corollary 6.3.6. Let $n \in \mathbb{N}$. Then, the Fibonacci number f_{n+1} is

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

This is precisely the phenomenon of Fibonacci numbers coming out if you add the entries of Pascal's triangle along certain slanted lines.

6.4. Compositions and weak compositions

6.4.1. Compositions

How many ways are there to write the number 5 as a sum of 3 positive integers, if the order matters?

$$\begin{aligned}
5 &= 1+2+2 = 2+1+2 = 2+2+1 \\
&= 3+1+1 = 1+3+1 = 1+1+3.
\end{aligned}$$

Six ways in total. What about the general case?

Definition 6.4.1. **(a)** If $n \in \mathbb{N}$, then a **composition of** n means 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** means a k-tuple of positive integers whose sum is n.

So we have just shown that the compositions of 5 into 3 parts are

$$(1,2,2)\,, \quad (2,1,2)\,, \quad (2,2,1)\,, \quad (3,1,1)\,, \quad (1,3,1)\,, \quad (1,1,3)\,.$$

The compositions of 3 are

$$(1,1,1)\,, \quad (2,1)\,, \quad (1,2)\,, \quad (3)\,.$$

The only composition of 0 is the empty list $()$, which is a 0-tuple and thus a composition of 0 into 0 parts.

Now let us count these compositions.

Theorem 6.4.2. 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 we furthermore have

$$(\#\text{ of compositions of } n \text{ into } k \text{ parts}) = \binom{n-1}{k-1}.$$

Proof. The case $n = 0$ is very easy, so we WLOG assume that $n > 0$.

Thus, $n - 1 \in \mathbb{N}$. We would like to construct a bijection

$$\begin{aligned} &\text{from } \{\text{compositions of } n \text{ into } k \text{ parts}\} \\ &\text{to } \{(k-1)\text{-element subsets of } [n-1]\}\,. \end{aligned}$$

This bijection sends each composition $a = (a_1, a_2, \ldots, a_k)$ to its **partial sum set**

$$C(a) := \{a_1,\ a_1 + a_2,\ a_1 + a_2 + a_3,\ \ldots,\ a_1 + a_2 + \cdots + a_{k-1}\}\,.$$

To see that this is really a bijection, we can (e.g.) construct its inverse as the map that sends each $(k-1)$-element subset S of $[n-1]$ to the composition

$$(s_1,\ s_2 - s_1,\ s_3 - s_2,\ \ldots,\ s_{k-1} - s_{k-2},\ n - s_{k-1})\,,$$

where $s_1, s_2, \ldots, s_{k-1}$ are the elements of S in increasing order.

Now that we have this bijection, we can use the bijection principle to obtain

$$\begin{aligned} &(\#\text{ of compositions of } n \text{ into } k \text{ parts}) \\ &= (\#\text{ of } (k-1)\text{-element subsets of } [n-1]) \\ &= \binom{n-1}{k-1} \qquad \text{(by the combinatorial interpretation of BCs)} \\ &= \binom{n-1}{(n-1)-(k-1)} \qquad \text{(by the symmetry of BCs)} \\ &= \binom{n-1}{n-k}. \end{aligned}$$

□

We can also count all compositions of n:

Theorem 6.4.3. Let n be a positive integer. Then, the # of all compositions of n is 2^{n-1}.

Proof. Same bijection as above, but without fixing k. The total # of subsets of $[n-1]$ is 2^{n-1}, as we know. □

6.4.2. Weak compositions

A **weak composition** is just like a composition, except that it allows its entries to be 0. In other words,

Definition 6.4.4. (a) If $n \in \mathbb{N}$, then a **weak composition of** n means 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** means a k-tuple of nonnegative integers whose sum is n.

For example, the weak compositions of 2 into 3 parts are

$$(1,1,0)\,, \quad (1,0,1)\,, \quad (0,1,1)\,, \quad (2,0,0)\,, \quad (0,2,0)\,, \quad (0,0,2)\,.$$

Counting all weak compositions of n is no longer a reasonable question, since there are ∞ of them: even just 0 has $()\,,\ (0)\,,\ (0,0)\,,\ (0,0,0)\,,\ \ldots$.

But we can count weak compositions of n into k parts:

Theorem 6.4.5. Let $n, k \in \mathbb{N}$. Then,

$$(\#\text{ of weak compositions of } n \text{ into } k \text{ parts}) = \binom{n+k-1}{n}.$$

Proof. There is a 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 is similar:

$$(b_1, b_2, \ldots, b_k) \mapsto (b_1 - 1,\ b_2 - 1,\ \ldots,\ b_k - 1)\,.$$

The bijection principle thus yields

$$\begin{aligned}
&(\#\text{ of weak compositions of } n \text{ into } k \text{ parts}) \\
&= (\#\text{ of compositions of } n+k \text{ into } k \text{ parts}) \\
&= \binom{n+k-1}{n+k-k} \qquad \text{(by a previously proved theorem)} \\
&= \binom{n+k-1}{n}.
\end{aligned}$$

□

6.5. Selections

We now come to a class of problems that we have mentioned a while ago but have not fully answered yet: How many ways are there to select a bunch of elements from a given set?

To be more specific: Given an n-element set S, how many ways are there to select k elements from it?

There are four ways to interpret this question, due to the following two choices:

1. Do we want k arbitrary elements or k distinct elements? ("With repetition" vs. "without repetition", aka "with replacement" vs. "without replacement".)
2. Does the order of these k elements matter or not? (That is, do "1, 2" and "2, 1" count as different choices or as one?)

Altogether you thus have 4 options, so 4 different counting problems. Let us address them all.

6.5.1. Unordered selections without repetition (= without replacement)

To choose k distinct elements from a given set S without regard to the order is just the same as choosing a k-element subset of S. The # of ways to do this is therefore

$$(\#\text{ of } k\text{-element subsets of } S) = \binom{n}{k}, \qquad \text{where } n = |S|.$$

6.5.2. Ordered selections without repetition (= without replacement)

To choose k distinct elements from a given set S with regard to the order is the same as choosing a k-tuple of distinct elements of S. I shall call such tuples **injective**. In other words:

Definition 6.5.1. 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 $i_a \neq i_b$ for all $a \neq b$).

For example, $(6, 1, 2)$ is injective, but $(3, 1, 3)$ is not.

Definition 6.5.2. Let S be any set, and let $k \in \mathbb{N}$. Then, S^k shall mean the Cartesian product

$$\begin{aligned}\underbrace{S \times S \times \cdots \times S}_{k \text{ times}} &= \{k\text{-tuples of elements of } S\} \\ &= \{(a_1, a_2, \ldots, a_k) \mid a_1, a_2, \ldots, a_k \in S\}.\end{aligned}$$

Now we claim:

Theorem 6.5.3. Let $n, k \in \mathbb{N}$. Let S be an n-element set. Then,

$$\begin{aligned}\left(\#\text{ of injective } k\text{-tuples in } S^k\right) &= n\,(n-1)\,(n-2)\cdots(n-k+1) \\ &= \binom{n}{k} \cdot k!.\end{aligned}$$

Informal proof. (See the notes for a rigorous version of this.)

Let us look at an example. Let $n = 5$ and $k = 3$ and $S = \{a, b, c, d, e\}$. How many injective k-tuples are there in S^k ? In other words, how many injective 3-tuples are there in S^3 ?

Such a 3-tuple has the form (x, y, z), where x, y, z are three distinct elements of S. Let us see how we can choose such a 3-tuple:

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 S has 5 elements but the element x is forbidden (because the injectivity of our tuple requires $x \neq y$).
3. Finally, we choose its third entry z. There are 3 options for this, since S has 5 elements but the elements x and y are forbidden (and x and y are distinct).

Altogether, we have 5 options at the first step, 4 options at the second, and 3 at the third. Each combination of these choices gives a different injective 3-tuple in S^3. So the total # of outcomes of this construction is $5 \cdot 4 \cdot 3 = 60$. What we have used here is a counting principle called the "**dependent product rule**", which (informally) says that if we perform a multi-step construction in which we have

- exactly n_1 options in step 1,
- exactly n_2 options in step 2,
- $\ldots$,
- exactly n_k options in step k,

then the entire construction can be performed in exactly $n_1 n_2 \cdots n_k$ many ways. Rigorously speaking, this is an induction argument on k.

So we got $5 \cdot 4 \cdot 3$ as an answer in our example. In the general case, the answer will be

$$n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right)$$

for the same reasons. But this equals $\dbinom{n}{k} \cdot k!$ because

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

□

6.5.3. Intermezzo: Listing n elements

If we apply the above theorem to $k = n$, then we conclude that the # of ways to choose n distinct from an n-element set, where the order matters, is

$$n\left(n-1\right)\left(n-2\right)\cdots\left(n-n+1\right) = n\left(n-1\right)\left(n-2\right)\cdots 1 = n!.$$

Of course, when we are choosing n distinct from an n-element set, we must necessarily choose all the elements of this set. So such a choice is simply an ordering of the n elements of our set. Thus, we have obtained the following:

Corollary 6.5.4. Let $n \in \mathbb{N}$. Let S be an n-element set. Then, the # of ways to list the elements of S in some order (i.e., the # of n-tuples that contain each element of S exactly once) is $n!$.

For example, for $n = 3$, these ways are

$$\left(1,2,3\right), \quad \left(1,3,2\right), \quad \left(2,1,3\right), \quad \left(2,3,1\right), \quad \left(3,1,2\right), \quad \left(3,2,1\right).$$

6.5.4. Ordered selections with repetition

How many ways are there to choose k elements of an n-element set S if the order matters? These ways are just the k-tuples in S^k, and they are easy to count:

Theorem 6.5.5. Let $n, k \in \mathbb{N}$. Let S be an n-element set. Then,

$$\left(\#\text{ of all } k\text{-tuples in } S^k\right) = n^k.$$

Proof. This follows from the product rule. □

6.5.5. Unordered selections with repetition

Only one of our four questions remains now: 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 concept of a **multiset**, which is "like a finite set but allowing for multiplicities" (i.e., an element can be contained a given # of times). This is normally done in Math 222.
2. Alternatively, we can define the concept of an **unordered k-tuple**, which is "a k-tuple up to reordering its entries". The formal way to do this is by using equivalence relations (unordered k-tuples are equivalence classes of k-tuples with respect to the equivalence of being permutations of each other).
3. Finally, the most pedestrian way: If S is a set of integers, then we consider the **weakly increasing** k-tuples of elements of S (i.e., the k-tuples $(s_1, s_2, \ldots, s_k)$ with $s_1 \leq s_2 \leq \cdots \leq s_k$).

These three definitions yield three different objects, but the # of them is always the same because there are bijections from one object to the other.

What is this #?

Theorem 6.5.6. Let $n, k \in \mathbb{N}$. Let S be an n-element set. Then,

$$\begin{aligned}&(\#\text{ of all ways to select } k \text{ elements from } S \text{ (if the order does not matter)})\\ &= \binom{k+n-1}{k}.\end{aligned}$$

Proof. See the notes. □

See the notes also for a few other combinatorial questions with answers.