Maths for Computer Science Positioning and Methodology MoSIG1

Denis TRYSTRAM
Denis.Trystram@univ-grenoble-alpes.fr
https://datamove.imag.fr/denis.trystram/teaching.php

August 29, 2023

Warm-up: motivation and use of Maths

Question:

What is Mathematics for you?

Warm-up: motivation and use of Maths

Question:

What is Mathematics for you?

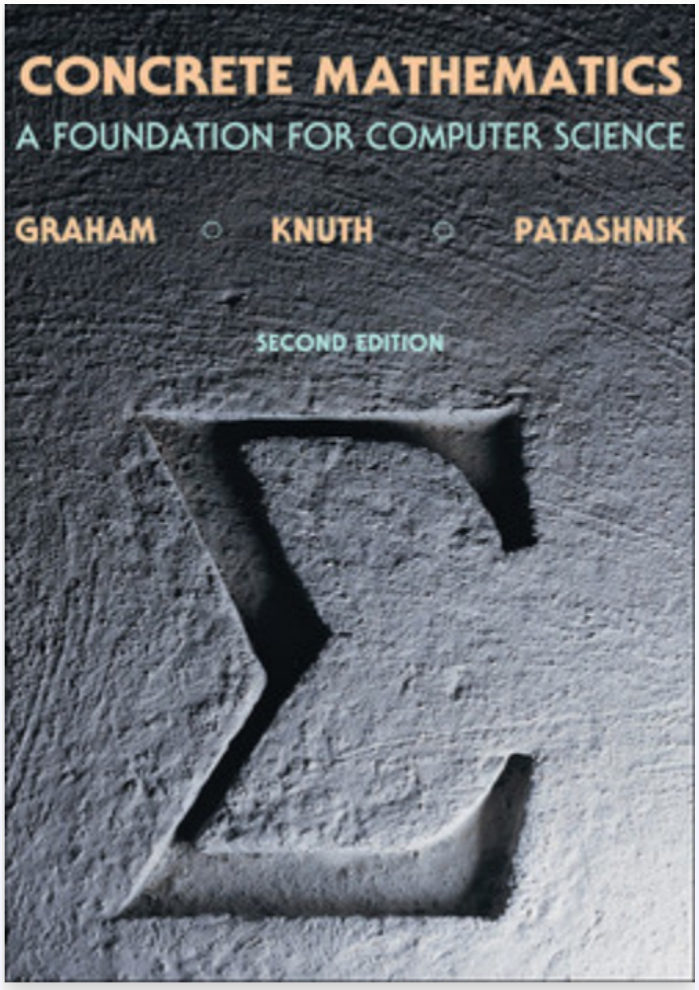
- Mathematics is a **Way of Thinking**

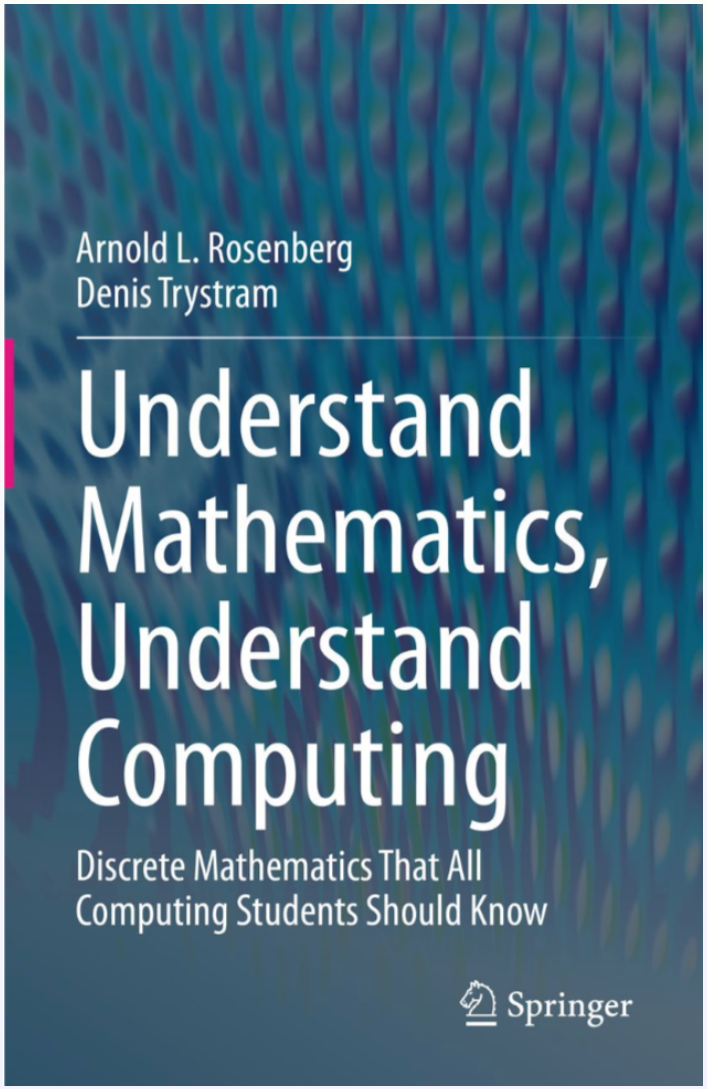
  People commonly think Maths as a collection of facts generated by a set of concepts enhanced by methods and tools for manipulating these concepts.

But it is much more!

Deep philosophical issues connect us to the ontological foundations (i.e., true nature) of *mathematical "objects"* such as functions, numbers, relations – and of the representational aspect of these objects – which *importantly* are what we compute with.

Bibliographic sources





Objectives of the training week

- **Deep understanding of the basic mathematical objects**:
  Study the true nature of these objects.
  Understand their ontological foundations.
- **Understand the mechanisms beyond mathematical reasoning**:
  formalization of the hypotheses
  defining the adequate notations
  logical decomposition of the steps
  writing proofs
- **Modelisation**:
  Going from a phenomenon (problem) to a formulation in mathematical language

Start by exemplifying mathematical "objects"

- An universal object: Set
- Functions
- Numbers
- Relations
- "Nothing" and infinity
- More specific constructions like
  logarithms, triangular numbers, binomial coefficients, $\cdots$

Set

Tentative definition

It is a fundamental object, easy to understand, but difficult to define precisely.
Actually, we don't need more.

- A set is a collection of *anything* you can imagine (could be students in a curriculum, odd integers, finite-length binary strings, etc.).
- Described by a rule or by the list of elements (in finite).
- We use various kinds of structure in sets to create complex objects that have sub-objects and sub-sub-objects, to arbitrary depths.
  Sub-sets (female students, primes, palindroms, etc.).

The main operations on sets

We focus first on the algebra that is built upon sets and the most basic operations on sets:

- *union* denoted by $S \cup T$, combines the membership of its argument sets, S and T
- *set difference* $S \setminus T$, excludes from set S all members of set T.

The main operations on sets

We focus first on the algebra that is built upon sets and the most basic operations on sets:

- *union* denoted by $S \cup T$, combines the membership of its argument sets, S and T
- *set difference* $S \setminus T$, excludes from set S all members of set T.

These two operations provide a *basis* for the algebra of sets, in the sense that one can combine these two operations in many different ways to craft an immense repertoire of operations on sets.

- As an example: define the following operation from union and set difference:
  intersection $(S \cap T)$, which isolates all elements shared by both sets S and T.

Extensions of sets

Structured sets:

- A rigorous analogue of the intuitive concept of *relation*.
  We can thenceforth talk about relations such as "parent-child", "set-subset", "numbers and their squares", and we can study how some of these relations behave like some others.
- *function* is among the central concepts of mathematics, and we identify valuable genres of function (one-to-one, onto, . . .).

Once we have these notions, we can begin to formulate *mathematical models* for real-life entities and situations.
Two features that will stand out: how naturally the formal notions capture the intuitive notions of the vernacular; how technically simple the formal notions are.

Functions

Definition

a function from a set S to a set S' is a *rule* that assigns a unique value from S' to every value from S.

Functions

Definition

a function from a set S to a set S' is a *rule* that assigns a unique value from S' to every value from S.

- This notion is a bit more restrictive than necessary.
  Think, for instance of the operation *division* on integers.
  - We learned at school that division is a function that assigns a number to a given pair of numbers – yet we are warned not to "divide by 0" since the quotient upon division by 0 is "undefined"
  - So, division is *not quite* a function of the same sort as addition or multiplication, which both *do* conform to the notion envisioned by the classical definition.

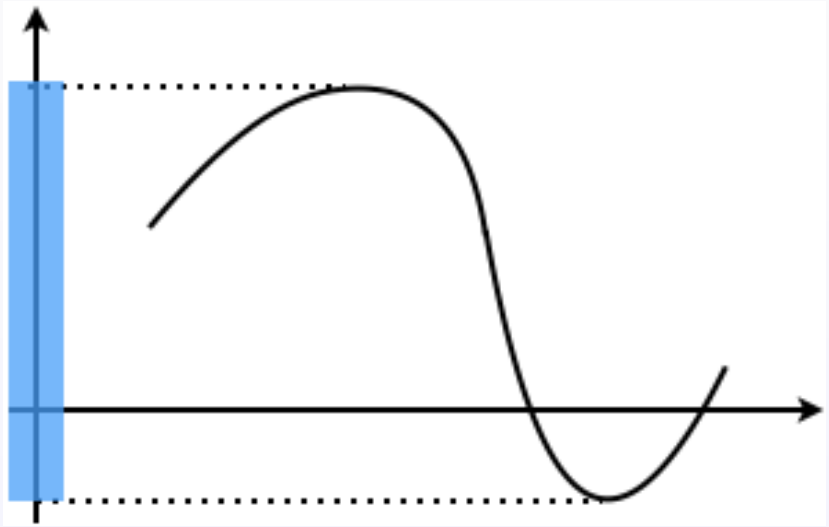
Injective functions

f is injective if for each $s' \in S'$, there is at most one $s \in S$ such that $f(s) = s'$

- "multiplication by 2" is injective:
  If you are given an even integer $2n$, you can always respond with the integer n.
- "integer division by 2" is not injective because performing the operation on arguments $2n$ and $2n + 1$ yields the same answer (namely, n).

Continuous versus Discrete

Intermediate values theorem for continuous functions



A discrete version

Two thieves Alice and Bob meet after a robbery. They want to share the loot (that is a necklace made of jewels) in a fair way.

Formal definition of the problem

Let us consider a necklace composed of an even number of jewels.

A discrete version

Two thieves Alice and Bob meet after a robbery. They want to share the loot (that is a necklace made of jewels) in a fair way.

Formal definition of the problem

Let us consider a necklace composed of an even number of jewels.

- Notation: $2n$ jewels ($2a$ rubies and $2b$ diamonds).

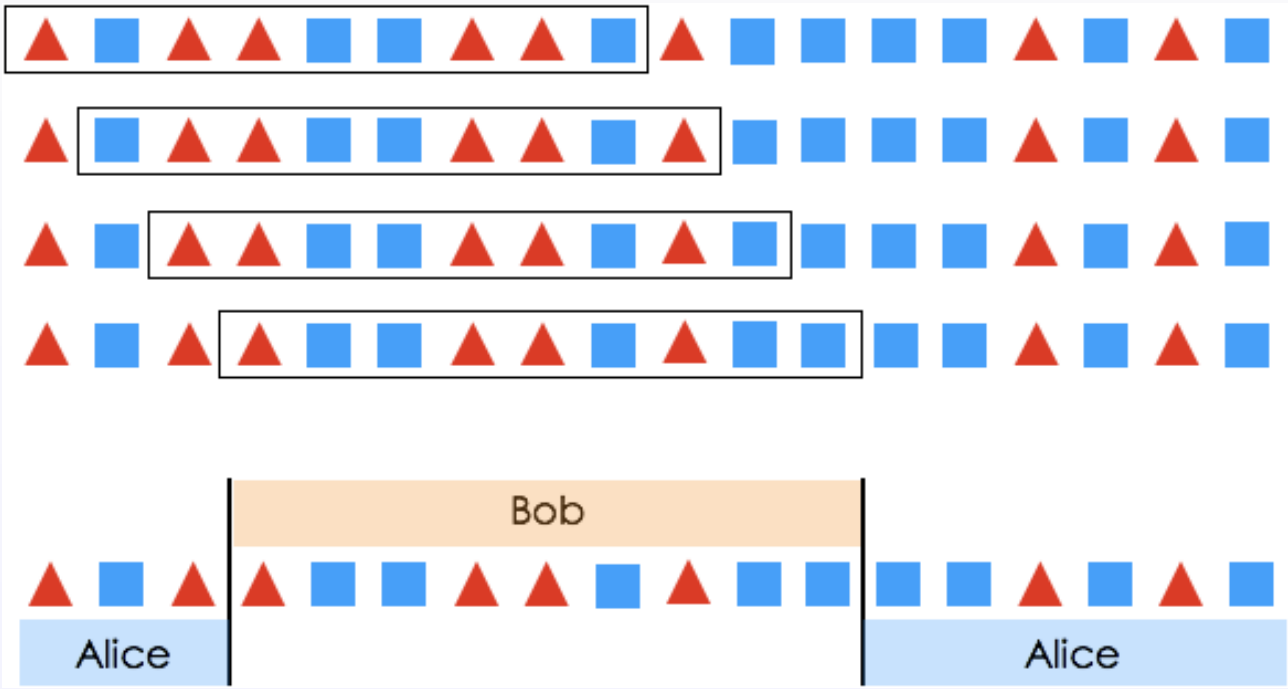
The problem is to determine a *fair* division while **cutting the necklace into several pieces of consecutive jewels with the minimum number of cuts**.

Analysis

- The problem can be solved in at most 2 cuts.
- Prove this result (constructive).

Analysis

- The problem can be solved in at most 2 cuts.
- Prove this result (constructive).



Formal Proof

The tube is (arbitrarily) put leftmost. We are going to shift right the tube, one jewel per step, and count the red and blue jewels at each step.
Of course, if there are currently equally many red inside the tube and outside, then, by simple arithmetic, we are done.
Otherwise, the tube currently has either too many red or too few.

- Say, with no loss of generality, that there are too many red inside the tube, namely, $a + c$ for some $c > 0$
  there is, therefore, a complementary number of blue jewels, namely, $b - c$[1].
- At the end of the process, the tube must contain a red jewels and b blue, the discrepancy c must have been reduced to 0.
  To see that this will eventually happen, we must characterize how c changes in a single step.

[1] there should be $a + b$ evenly in each side

The effect of a single shift is to insert a jewel into the tube, at its right, and to eliminate a jewel from the tube, at the left.

The discrepancy can be changed in precisely three ways.

- If the inserted jewel and the eliminated jewel are of the same color, then the discrepancy c is unchanged.
- If the inserted jewel is red and the eliminated jewel is blue, then the discrepancy c is *increased to* $c + 1$ by this shift.
- If the inserted jewel is blue and the eliminated one is red, then the discrepancy c is *decreased to* $c - 1$.

The effect of a single shift is to insert a jewel into the tube, at its right, and to eliminate a jewel from the tube, at the left.

The discrepancy can be changed in precisely three ways.

- If the inserted jewel and the eliminated jewel are of the same color, then the discrepancy c is unchanged.
- If the inserted jewel is red and the eliminated jewel is blue, then the discrepancy c is *increased to* $c + 1$ by this shift.
- If the inserted jewel is blue and the eliminated one is red, then the discrepancy c is *decreased to* $c - 1$.

By the time n shifts have been performed, the discrepancy c will have changed to $-c$, because the tube will be in an antipodal position upon the necklace.

Summarize

- Over the course of n shifts, the discrepancy c will have changed to $-c$.
- The discrepancy changes by ± 1 at each shift.
- Therefore, there must be some shift among the n when the discrepancy is 0.

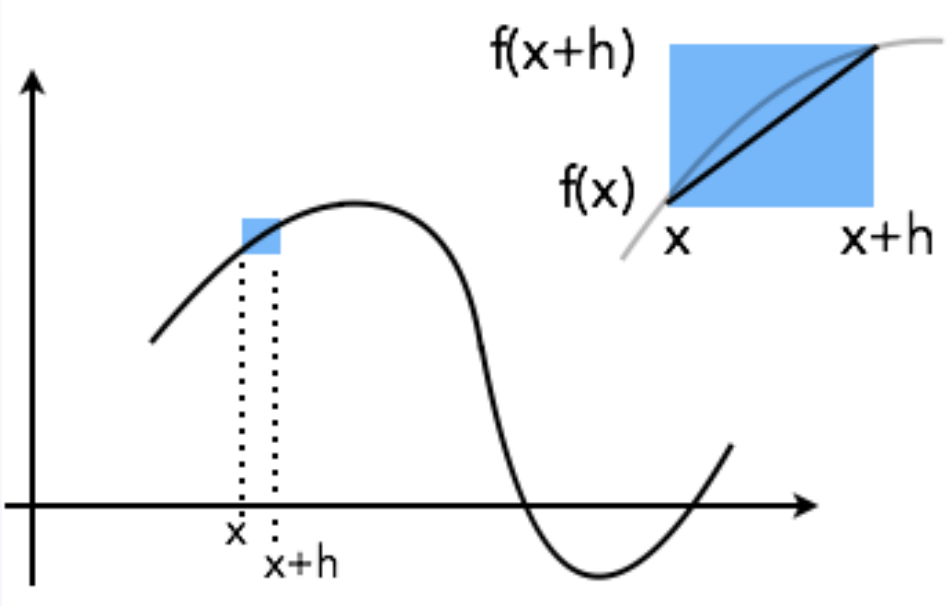
Lesson learned

Notations are a prerequisite for any mathematical analysis.

- They help to identify the key parameters (Occam razor).
- Clear and explicit notations help to derive the proofs.

Derivatives

Consider a continuous function.



$$f'(x) = lim_{h \to 0}[\frac{f(x+h)-f(x)}{h}]$$

Classical (and useful) derivatives

- Polynomials
- Exponentials and logarithms.

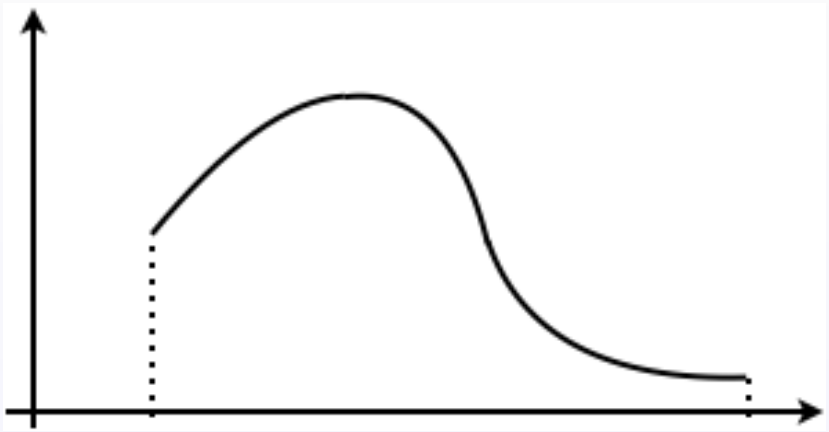
Integrals

Integration is the reverse operation of derivatives.

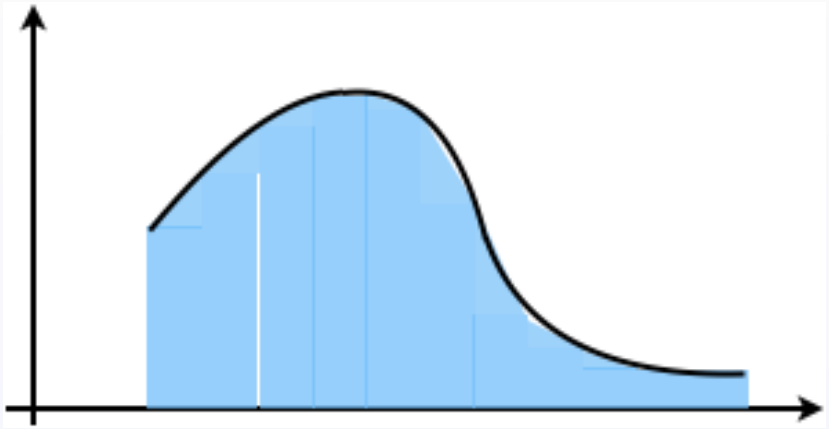
Integrals are continuous by nature, but they can be calculated by (discrete) Riemann's sums – defined as areas under enveloping continuous functions.

Definition

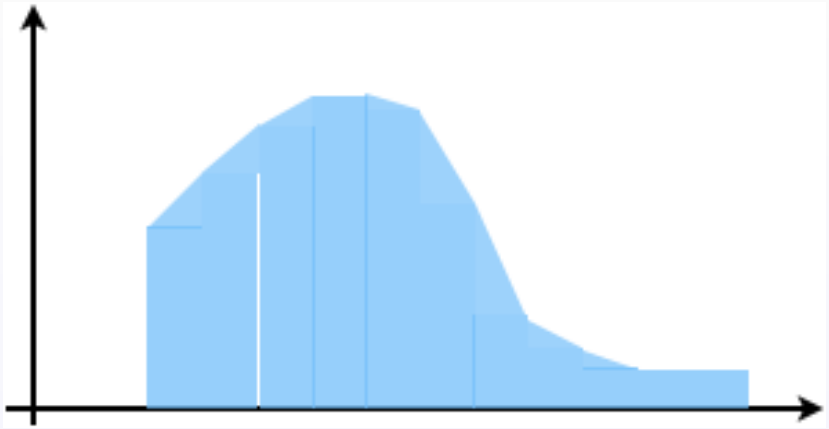
Let consider a positive function.



Its integral is the surface below the function



Choice of a step (arbitrarly small)



In action...

The stratagem follows a three-step procedure.
Focus on a summation we want to determine

$$S = a_1 + a_2 + \cdots + a_n$$

We have specified S as a *finite* summation to simplify exposition[2].

[2] It also works with infinite summations

Example on the summation S

Step 1. Represent the summands of S as a series of n abutting (unit-width) rectangles of respective heights $a_1,\ a_2, \ldots,\ a_n$.

Step 2. Construct a continuous curve $\overline{C}(x)$ that passes through the corners of the rectangles, in such a way that they lie completely within the area under $\overline{C}(x)$.

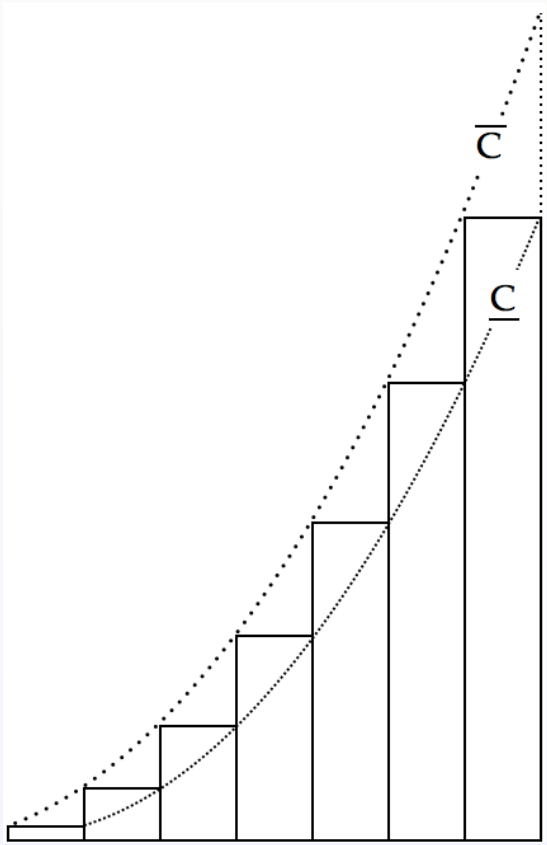
The area under the curve $\overline{C}(x)$ – obtained by integrating $\overline{C}(x)$ between appropriate limits – yields an *upper bound* of S.

Step 3. Construct another continuous curve $\underline{C}(x)$ that also passes through the corners of the rectangles, such that the area under $\underline{C}(x)$ lies completely within the rectangles.

The area under the curve yields a *lower bound* of S.

Integrals (in action)

$S_2(n) = \sum_{i=1}^{n} i^2$, for $n = 7$



The area under curve $\underline{C}$ is $A(\underline{C}(x)) = \int_1^n x^2 \mathrm{d}x$.

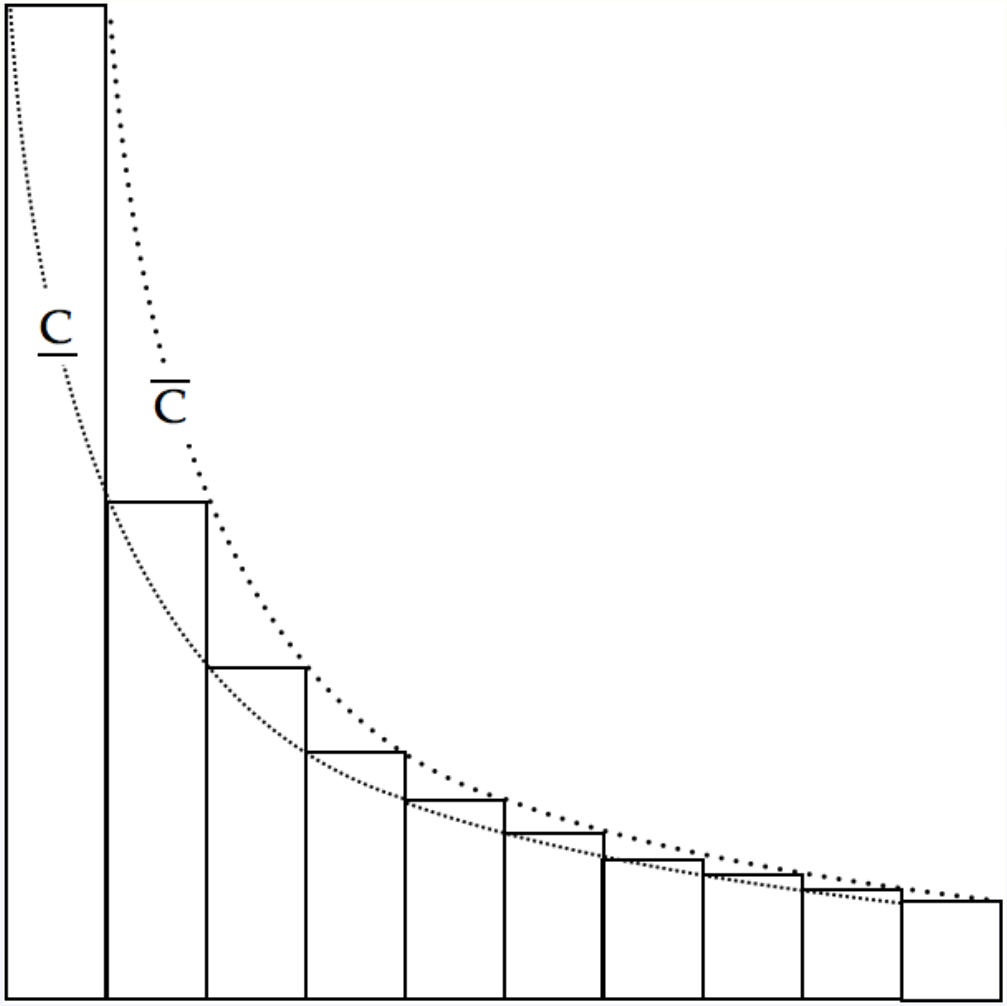
Another example

- Harmonic series and the logarithm function

$$S^{(H)}(10) = \sum_{i=1}^{10} i^{-1} = \sum_{i=1}^{10} 1/i =$$

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10}$$

Derivative of log(x) $= \frac{1}{x}$


C
C

Numbers

Being used for elementary operations such as counting, the integers are almost certainly the first numbers that our prehistoric ancestors would have used.

The Number Line

Let us survey briefly the most important properties of the following three sets, which collectively comprise "the integers".

- The set Z comprises *all integers* – the positive and negative integers plus the special number zero (0).
- The set N comprises the *nonnegative integers* – the positive integers plus zero (0).
- The set N^+ comprises the *positive integers*.

Operations on numbers

Several essential properties of the sets Z, N, and N^+ are consequences of the integers' behaviors under their natural *order* relations:

- the two *less-than* relations:
  - the *strict* relation ($<$).
  - the *non-strict* or *weak* relation ($\leq$).
- their *converses*, the *greater-than* relations:
  - the *strict* relation ($>$).
  - the *non-strict* or *weak* relation ($\geq$).

Rationals

Each enrichment of our number system throughout history has been a response to a deficiency with the then-current system. The deficiency that instigated the introduction of the rational numbers was the fact that many integers do not divide certain other integers.

This situation led to practical problems when people began to share commodities that were physically divisible[3]

[3] With a bit of care, you can always cut a pizza into any desired number of slices

Properties

The set Q of *rational* numbers was invented to name the quotients referred to in the preceding paragraph.

Formally: $Q \equiv 0 \cup [p/q \mid p, q \in Z \setminus 0]$
Each *nonzero* rational number p/q is often called a *fraction*.
In analogy with our treatment of integers, we reserve the notation Q^+ for the *positive* rationals.

An alternative, mathematically more advanced, way of defining Q is as *the smallest set of numbers that contains the integers and is closed under the operation of dividing any number by any nonzero number.*
The word "*closed*" here means that, for every two numbers $p \in Q$ and $q \in Q \setminus \{0\}$, the quotient p/q belongs to Q.

A *tool* for comparison

There are many ways to compare the sets Z and Q that enhance our understanding of both sets.

As the first point in our comparison, we remark that every integer $n \in Z$ can be encoded as a rational number.

- Specifically, we represent/encode the integer $n \in Z$ by the rational p/q whose numerator is $p = n$ and whose denominator is $q = 1$.

This encoding is so intuitive that most people would write "$n = n/1$" and ignore the fact that this is expressing an encoding rather than an equality. We know with hindsight that this intellectual shortcut can cause no problems, but it is important to be aware of this.

Arithmetic operations

The arithmetic operation *multiplication* was surely recognized not long after its slightly simpler sibling operation *addition*.
In many ways, these two operations mimic one another.

Let us prove the following expression:

$$\Sigma_{k=1,n}(k^2(k+1) - k(k-1)^2) = n^2(n+1)$$

The idea here is first to test your ability to manipulate numbers and second, to figure out how to write a simple proof.

Proof 1

To get insight, let start by the small values of n.

- $n = 1$, $(1^2(1+1) - 1(1-1)^2) = 1^2(1+1)$
- $n = 2$,
  $1^2(1+1) - 1(1-1)^2) + 2^2(2+1) - 2(2-1)^2) = 2^2(2+1)$

In both cases, we see that the sum reduces to a single term...

The basic insight comes by remarking that the result we are looking for (i.e. the right hand side) is contained into the summation, more precisely, this is the first term with $k = n$.

Proof 2

The summation can be written as follows:
$n^2(n+1) + \Sigma_{k=1,n-1}(k^2(k+1) - \Sigma_{k=1,n}k(k-1)^2)$

Now, let us also remark that the second can be simplified since the first term is nul for $k = 1$:
$\Sigma_{k=2,n}k(k-1)^2$

Let shift the indices in this sum (change k to $k' = k+1$):
$\Sigma_{k'=1,n-1}(k'+1)k'^2$.

This concludes the proof since both summations are the same.

Both are *total bivariate functions* which take a pair of numbers and produce a number; both are:

- *commutative*, in that the argument numbers can be presented in either order without changing the result
- and *associative*, in the sense asserted by the equations

$$(\forall a, b)\ \big[[a{+}(b{+}c)\ =\ (a{+}b){+}c]\quad \text{and}\quad [a{\cdot}(b{\cdot}c)\ =\ (a{\cdot}b){\cdot}c]\big]$$

If we restrict to the *integers*, however, there is a glaring difference: addition has a "partner operation", *subtraction*, which operates as an *inverse operation*:

$$(\forall a, b, c)\big[\text{if}\quad [c = a + b]\quad \text{then}\quad [a = c - b]\big]$$

Reals

Real numbers are somehow an equivalent of continuous numbers.

Definition of irrationals

Numbers that can not be written as the ratio of two integers.

Example

Computing $\sqrt{2}$

- Negative results are usually harder to establish than positive (constructive) ones.

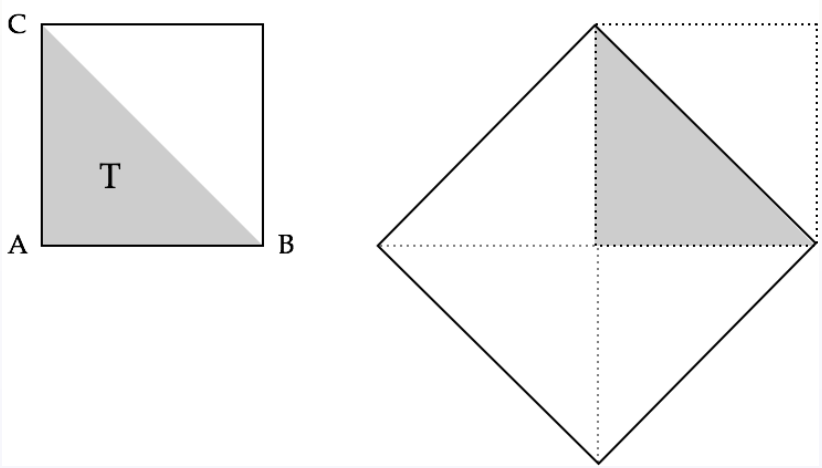
Pythagorean construction

The Greek mathematician Euclid verified the uncomfortable fact that the lengths of portions of eminently buildable structures were not measurable.
The poster child for this phenomenon was the *hypotenuse of the isosceles right triangle T with unit-length sides*.
Thanks to the well-known theorem of Pythagoras, even schoolchildren nowadays know that the length of this eminently "buildable" (with straightedge and compass) line is $\sqrt{2}$. What Euclid discovered is:

There is – provably – no way to find integers p and q whose ratio is $\sqrt{2}$, the length of T's hypotenuse.

Pythagorean theorem 1

Let us be given a triangle T with vertices A, B, and C.
Use the left-hand grey triangle as a model.



Say that T is a *right triangle*, meaning that one of its angles is a *right angle*. The line from B to C is called the *hypotenuse* of T. T has a very special shape: it is *isosceles*, meaning that its two sides have the same length.

The grey triangle is an isosceles right triangle.

Pythagorean theorem 2

Theorem

Let T be a right triangle whose two sides have respective lengths s_1 and s_2, and whose hypotenuse has length h. Then

$$h^2 = s_1^2 + s_2^2$$

Consequently, when T is an *isosceles* right triangle, then $h^2 = 2s_1^2$ and if $s_1 = 1$, thus, $h = \sqrt{2}$

In the previous construction, the diagonal of the unit-side square is the hypotenuse of the two triangles.
we use the partitioned to construct a new, bigger square whose side-length is the hypotenuse of T.

- The grey triangle has area $1/2$ since it is half of the unit square.
- Thus, the area of the big square is 4 times more: $4 \cdot (1/2) = 2$.

Because the hypotenuse of the grey triangle is a side of an area-2 square, the hypotenuse of the unit-side isosceles right triangle is $\sqrt{2}$.

In the previous construction, the diagonal of the unit-side square is the hypotenuse of the two triangles.
we use the partitioned to construct a new, bigger square whose side-length is the hypotenuse of T.

- The grey triangle has area $1/2$ since it is half of the unit square.
- Thus, the area of the big square is 4 times more: $4 \cdot (1/2) = 2$.

Because the hypotenuse of the grey triangle is a side of an area-2 square, the hypotenuse of the unit-side isosceles right triangle is $\sqrt{2}$.

We will prove formally the irrationality in the lecture next week.

Binary and hexadecimal integers

Consider the decimal[4] 2023

- $2023 = 1024 + 512 + 256 + 128 + 64 + 32 + 8 + 2 + 1$
  thus, the binary writing is: $(11111101011)_2$
- $2023 = 7 \times 16^2 + 231$ and $231 = 14 \times 16 + 7$
  thus, the hexadecimal writing is: $(7, 14, 7)_{16}$

[4] decimal means in basis 10

Nothing and infinity

- What is “nothing”?
  How does the concept *zero* represent “nothing”?
  Are there multiple candidates for a *zero*, which capture this concept in distinct ways?
- At the other end of the spectrum, what is “infinity”?
  In what ways does infinitude differ from finitude? Is there more than one valid — i.e., logically consistent — notion of “infinity”?

Infinitesimal calculus

The notion of *infinitesimals*, as invented by Newton and Leibniz, explains the fallacy of assertions such as the Tortoise's Zeno paradox.
This notion, which plays a huge role in modern mathematics, underlying such foundational concepts as *limits* and *continuity* (of functions), was not well understood until just a few hundred years ago.

The general topic of the convergence or divergence of infinite series is beyond the scope, but we shall observe several examples of each concept like the infinite summation $\frac{1}{k}$

Proof of divergence

$$S^{(H)} = \sum_{k=1}^{\infty} \frac{1}{k}$$

Principle

1. Partition $S^{(H)}$'s terms into groups whose sizes are successive powers of 2
2. Develop an argument based on the sums within the groups.

The partitioning step operates as follows:

$$S^{(H)} = 1 + \tfrac{1}{2} + \left(\tfrac{1}{3} + \tfrac{1}{4}\right) + \left(\tfrac{1}{5} + \tfrac{1}{6} + \tfrac{1}{7} + \tfrac{1}{8}\right) + \left(\tfrac{1}{9} + \tfrac{1}{10} + \tfrac{1}{11} + \tfrac{1}{12} + \tfrac{1}{13} + \tfrac{1}{14} + \tfrac{1}{15} + \right.$$

In detail, each group, say the ith group G_i (for $i \geq 1$), is computed from the i numbers

$$\frac{1}{2^{(i-1)}+1}, \ \frac{1}{2^{(i-1)}+2}, \ \cdots, \ \frac{1}{2^i}$$

Grouping the terms in the earlier manner, the sum within each group G_i exceeds $1/2$:

$$\begin{aligned}
\frac{1}{3} + \frac{1}{4} &> 2 \cdot \frac{1}{4} = \frac{1}{2} \\
\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} &> 4 \cdot \frac{1}{8} = \frac{1}{2} \\
\frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} + \frac{1}{16} &> 8 \cdot \frac{1}{16} = \frac{1}{2} \\
&\vdots
\end{aligned}$$

Therefore,

$$\begin{aligned} S^{(H)} &> 1 + \left(\frac{1}{2} + \frac{1}{2}\right) + \left(\frac{1}{2} + \frac{1}{2}\right) + \cdots \\ &= 1 + 1 + 1 + 1 + \cdots \end{aligned}$$

This means that the Harmonic sum $S^{(H)}$ is greater than every sum of 1s and hence is infinite.

Remark: We may propose an alternative analysis of the same result by using groupings whose sizes are multiples of 3 in $S^{(H)}$.

From finite summations to infinite

- Dealing with limits

Asymptotic notations

- upper bound
  $f = O(g) \Leftrightarrow \exists C > 0\ \exists n_0 > 0\ \forall n > n_0\ f(n) \leq Cg(n)$
- lower bound
  $f = \Omega(g) \Leftrightarrow g = O(f)$
- $f = \Theta(g) \Leftrightarrow f = O(g)$ and $f = \Omega(g)$

From finite summations to infinite

- Dealing with limits

Asymptotic notations

- upper bound
  $f = O(g) \Leftrightarrow \exists C > 0\ \exists n_0 > 0\ \forall n > n_0\ f(n) \leq Cg(n)$
- lower bound
  $f = \Omega(g) \Leftrightarrow g = O(f)$
- $f = \Theta(g) \Leftrightarrow f = O(g)$ and $f = \Omega(g)$

take care! The "equals sign" in the notation $f(x) = O(f(x))$ does *not* mean "equals".

Order of magnitude of common functions

Classify asymptotically the following functions
(variable n – integer).

$$log(n) \qquad 2^n \qquad \sqrt{n} \qquad n^n \qquad log(log(n)) \qquad n^3$$

Order of magnitude of common functions

Classify asymptotically the following functions
(variable n – integer).

$$log(n) \qquad 2^n \qquad \sqrt{n} \qquad n^n \qquad log(log(n)) \qquad n^3$$

- They are all non-decreasing functions
- The *hierarchy* (from small to large) is the following:

$log(log(n))$, $log(n)$, $\sqrt{n}$, n^3, 2^n, n^n.

Two examples for dealing with infinity

- The Zeno paradox
- A first puzzle:
  "les douze coups de minuits..."
- Going further: Hilbert's hotel

Achille and the tortoise

In Zeno's story, the slow-footed Tortoise (T) tries to convince the speedy Achilles (A) of the futility of trying to win any race in which A gives T even the smallest head start.

- As long as T is ahead of A, says T, every time A traverses half the distance between himself and T, T will respond by moving a bit further ahead.
- Thereby, T will always be a positive distance ahead of A, so that A can *never* catch T.

The resolution of the apparent paradox resides in the notion of *infinitesimals* – quantities that dynamically grow smaller than any finite number.

A first thought about large infinity

What is the value of $1 - 1 + 1 - 1 + \cdots$?

At the new year party

Close to midnight, people are a bit drank, they propose a game.

- Take an arbitrarily large hat and a collection of n (infinite number) of small balls.
- The game consists in filling the hat as follows:
  - at midnight-30 seconds, put 10 balls into the hat
  - at midnight minus 15 sec., remove one ball and fill the hat with the next 10 balls
  - and so on at midnight minus $\frac{30}{4}$, $\frac{30}{8}$, ... until midnight rings
- The question is:
  "How many balls are into the hat at midnight?"

There is no canonical answer!

Hilbert's hotel

- Consider an hotel with an infinite number of rooms, say n, the rooms can be indexed over the integers.
- All rooms and occupied
- A new guest arrives
- As n is infinite, we can shilft **all** the persons of rooms i to the next $i + 1$
  thus, room 1 is idle and it can accommodate the new guest.

Hilbert's hotel (2)

Even more

We may extend the previous argument for an infinite number of new guests by assigning room i to room $2i$.

There are "equally many" integers within the set N of *all* integers as there are in

- N's proper *subset* that comprises just the *odd* integers.
- N's proper *superset* that comprises ordered pairs of integers.

Does this mean that "infinite is infinite", i.e., that one can match up the elements of any two infinite sets.

Synthesis

- Infinity usually refers to a simple question with multiple answers
- The classical arithmetic operations do not hold anymore at infinity

Message

We can not perform classical arithmetic operations at infinity!

Coming back to a fondamental question

A crucial step in doing mathematics can be termed *modeling*.

Developing mechanisms for explicit reasoning:

- Formalizing hypotheses
- Define adequate notations
- Decomposing complex phenomena into simpler components
- Making the logical inferences that ultimately lead one to mathematical proofs about real phenomena