Ideas of mathematical proof

Slides Week 19

Information about the module. Introduction. Mathematical induction. Recursive definitions.

Information about the module

MTH1003

Ideas of Mathematical Proof

Teaching delivery:

- Mostly 3 hours lectures and 1 hour practical per week, apart from Weeks 19, 23, and 30 with 4 hours lectures.

  Week 26: 'light teaching', no lectures, nor practical.

  Week 33: four hours revision classes only.

- Recall: at practicals solving problems, under the lecturer's supervision. Collaboration with other students is allowed, and you are welcome to ask the lecturer for help.

- A problem sheet uploaded before practical.
  Best if students work on the questions beforehand and ask pertinent questions in class.

  No assessment associated with practicals.

- Often not enough time for all questions: take home and try independently what was not done in class.

- Later full solutions uploaded on Blackboard.
  At the very least read and understand all the solutions.

Primary learning materials:

- Slides are made available on Blackboard, often preliminary version before the lecture.

  Advice/requirement: attendance essential.

- Questions for each practical (solutions afterwards) will be on Blackboard.

- Lectures and problem sheets (and individual study) should be enough to study the module.

Recommended books:

- J. Taylor *Understanding mathematical proof*, CRC Press, 2014 (copies in the library).
- P. Eccles, *An introduction to mathematical reasoning: numbers, sets, and functions*, Cambridge University Press, 1997, 2007 (copies in the library).

These books (or other books or sources) can be used for additional exercises, deeper insight into the subject.

Warning: Exposition/notation, etc., may be different in different books.

Assessment:

- Portfolio: one coursework Assignment (15%) and Mid-Term In-Class Test (25%).
- Exam (60%) in May-June.
- Portfolio $= 40\%$ of the final mark, exam $= 60\%$.
- Assignments deadlines:

	Issued	Hand in	Feedback
C/W Assign.	22/02/2024	29/02/2024	12/04/2024
In-Class Test	14/03/2024		04/04/2024

Coursework is to be submitted via Turnitin by 3pm.

Each day of delay penalised -10% of the total marks.

0. Introduction

Interconnections between applications of mathematics and mathematical theories.

New maths is often created as a response for the needs of other sciences.

Conversely, pure maths created earlier finds applications.

In Ancient Egypt, loops of rope with 12 knots at equal distances were used to delineate rectangular pieces of land: such a loop arranged as a triangle with sides 3, 4, 5 gives a right angle, since $3^2 + 4^2 = 5^2$. Pythagoras theorem: $a^2 + b^2 = c^2$ for sides of a right triangle. But here it is actually converse theorem that 'works': if $a^2 + b^2 = c^2$, then it is right angle opposite side c.

Pythagoras and non-Euclidean geometry

Pythagoras theorem **was proved** in ancient Greece 2000 years ago.

But pure mathematicians continued to analyse the **proof**, how it is derived from Axioms, Postulates.

This was of purely theoretical interest. As a result, non-Euclidean geometry was discovered about 200 years ago, which was still very theoretical, 'imaginary'.

But 100 years later it became important for Relativity Theory in physics.

'Main theorem' of calculus

Calculus first appeared as a tool for mechanics: velocities, distances, acceleration, etc.

When we integrate, say, $\int_a^b x^3 dx = b^4/4 - a^4/4$,

we are using the **Newton–Leibnitz theorem**:

if $F'(x) = f(x)$, then $\int_a^b f(x)dx = F(b) - F(a)$,

or: $\dfrac{d\int_a^z f(x)dx}{dz} = f(z)$.

This theorem is quite nontrivial; had to be **proved**.

More examples

- Kepler's discovery: orbits of planet are ellipses. Must have had an **idea** of ellipse – a conic section, in mathematical theory since Ancient Greece.
- Quantum physics required invention of new type of functions (like delta-function), so-called distributions, or generalized functions, operator theory.
- Number theory used to be very pure maths, now it is very much applied, in cryptography.
- Fourier transforms developed in maths 200 years ago are used in modern signal processing (digital music, radio, television, mobiles).

Rigour

Mathematics now has reputation as most rigorous of all sciences, with 'absolute' proofs.

Mathematical proof of a theorem must be a 'tree' (without cycles!), starting from axioms, from which everything is derived by precise rules of inference.

Everything in maths must have a precise definition.

Early example of axiomatic theory is Euclidean geometry.

Example

$\lim_{x\to 0} \frac{\sin x}{x}$? l'Hôpital's rule? $(\sin x)' = \cos x$ and $x' = 1$;

then $\lim_{x\to 0} \frac{\sin x}{x} = \lim_{x\to 0} \frac{\cos x}{1} = \frac{\cos 0}{1} = \frac{1}{1} = 1.$

But for proving that $(\sin x)' = \cos x$

we actually need precisely this limit $\lim_{x\to 0} \frac{\sin x}{x}$.

in Latin: *circulus in probando*, "circle in proving": "A is true because B is true, and B is true because A is true" – thus one can 'prove' anything!

(Usually $\lim_{x\to 0} \frac{\sin x}{x} = 1$ is proved first, by geometric argument, or otherwise, only after that $(\sin x)'$...)

Calculus before rigour

Calculus first appeared in 16–17 centuries
with imprecise definitions of limits, derivatives, integrals.

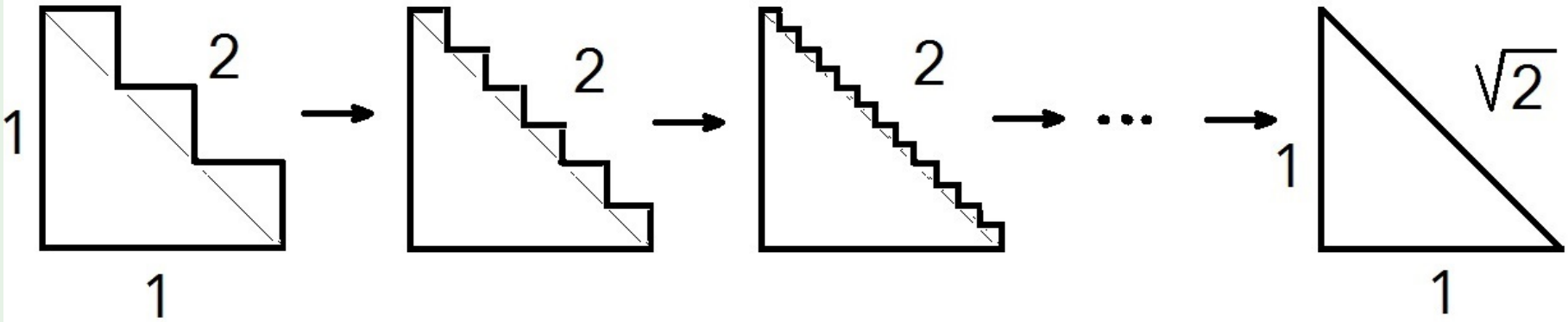
So-called infinitesimals were used (infinitely small quantities).

Mathematicians relied on their intuition to avoid errors (not always successfully).

A simple example of improper use of limits:

Example

Making zigzag 'steps' ever smaller, we make the zigzag line approach in the limit the hypotenuse.



At every step the length of the zigzag line is 2:
the sum of all horizontal pieces is 1,
and the sum of all vertical pieces is 1.

Then 'surely' the length of the limit – the hypotenuse – must be the limit of these lengths: $\lim 2 = 2$.

We obtained $2 = \sqrt{2}$?!

Rigorous foundations of mathematics

Only in 19th century precise definitions of limits, derivatives, integrals were given and rigorous foundations of calculus were established.

Set theory emerged in late 19th century, nowadays is the language in which all maths is written, defined.

Mathematical logic

In 19th century mathematical logic appeared, which analyses the very process of mathematical reasoning.

(George Boole, 1815–1864, in Lincoln! was a pioneer of mathematical logic.)

Mathematical logic was one of the most pure, theoretical parts of maths.

Now it is language of computer science.

Even in computer hardware: so-called Boolean logical gates – semiconductor switches – form computer circuits.

Imagination, inspiration, ingenuity, experiment, intuition

are all required in maths, in order to achieve results.

The end result in maths must be precise, rigorous, well defined, proved.

But inner workings of a mathematician's mind are of course not formal proofs.

As Hilbert (one of the greatest mathematicians) said about one of his former pupils: "*You know, for a mathematician, he did not have enough imagination. But he has become a poet and now he is fine.*"

Module contents

1. Mathematical induction.
2. Sets, relations, mappings, cardinalities.
3. Elements of mathematical logic.
4. Rigorous definitions of limits.

See more detailed contents on Blackboard.

Notation, abbreviations: numbers.

$\mathbb{N}$ is (the set of all) positive integers,

$\mathbb{Z}$ – integers,

$\mathbb{Q}$ – rational numbers,

$\mathbb{R}$ – real numbers,

$\mathbb{C}$ – complex numbers.

Notation, abbreviations: sets.

A set is denoted by braces: $\{\dots\}$, with elements specified in some way.

E.g. $\mathbb{N} = \{1, 2, 3, \dots\}$.

We write $a \in A$ to denote "a is an element of A" (or a belongs to A).

E.g. $3 \in \mathbb{N}$, $0.5 \notin \mathbb{Z}$, $2/3 \in \mathbb{Q}$, $\sqrt{3} \notin \mathbb{Q}$.

Set defined by some property: $\{x \mid P(x) \text{ is true}\}$, read: "the set of all x such that $P(x)$ is true".

E.g. $\{x \in \mathbb{R} \mid 1 \leq x \leq 2\}$ is the interval $[1, 2]$.

(Notation varies! often colon is used instead of $|$, like $\{x : P(x) \text{ is true}\}$.)

Notation, abbreviations: logic.

$\forall$ abbreviates "for all", "every", etc.

$\exists$ abbreviates "there exists", "there is".

(These symbols, quantifiers, have special precise meaning in math. logic, but for the moment these are just abbreviations for slides/whiteboard/solutions, etc.)

$\Rightarrow$ abbreviates "implies". So if P and Q are two statements, $P \Rightarrow Q$ means "P implies Q", the same as "Q follows from P", etc.

E.g. $x > 2 \Rightarrow x^2 > 4$, but $x^2 > 4 \not\Rightarrow x > 2$.

1. Mathematical induction

Axiom of Mathematical Induction

Mathematical induction is about statements depending on positive integers. Axiom of Mathematical Induction is part of basic axioms (assumed without proof) on which all mathematics is based.

Axiom of Mathematical Induction.

Suppose that $P(n)$ is a proposition, or property, depending on a positive integer $n \in \mathbb{N}$. Suppose that

1° $P(1)$ is true, and

2° if $P(k)$ is true, then $P(k+1)$ is true.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

(Notation 1°, 2° is traditional, called the base of induction and the induction step.)

$P(1)$ is true by $1^\circ \Rightarrow P(2)$ is true by $2^\circ \Rightarrow P(3)$ is true by $2^\circ \Rightarrow P(4)$ is true $\Rightarrow P(5)$ is true $\Rightarrow P(6)$ is true, and so on...

Remark: We consider simple problems as examples. Some can be solved without mathematical induction. But we use induction to exercise, even if there is a simpler solution.

Example

Prove by induction the formula

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

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

First we check the base of induction:

1°. For $n = 1$ we have $1 = \dfrac{1(1+1)}{2}$, true.

2°. Now we assume that the formula is true for $n = k$, that is, we **assume** that

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

and want to prove that **then** the formula is also true for $n = k + 1$, that is, we want to derive

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

(advantage: we can **use** the formula for $n = k$).

On the left we substitute $\frac{k(k+1)}{2}$ for $1+2+\cdots+k$ using our assumption (usually called the induction hypothesis):

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

$$= \frac{k^2+k+2k+2}{2} = \frac{k^2+3k+2}{2}.$$

The right-hand side for $n = k+1$ is

$$\frac{(k+1)((k+1)+1)}{2} = \frac{k^2+2k+1+k+1}{2} = \frac{k^2+3k+2}{2},$$

the same, as required. We have proved the induction step.

By Axiom of Mathematical Induction (AMI) now 1° & 2° imply that the formula is true for all $n \in \mathbb{N}$:

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \text{ for all } n \in \mathbb{N}.$$

Remark: when deriving for $n = k + 1$ there is no need to transform the l.h.s. exactly to the form of the r.h.s. Just prove equality l.h.s.= r.h.s by any method (using the induction hypothesis), like above we reduced both l.h.s. and r.h.s. to the same expression (but transformations must be reversible, so that true equality at the end really implies the previous ones...).

Recall: "an integer a is divisible by an integer b" by definition means that $a = bk$ for some integer $k \in \mathbb{Z}$.

Example

Prove by induction that $3^{2n} + 7$ is divisible by 8 for any $n \in \mathbb{N}$.

1°. For $n = 1$ we have $3^{2 \cdot 1} + 7 = 9 + 7 = 16$

is divisible by 8, true (since $16 = 8 \cdot 2$).

2°. Assume that this is true for $n = k$, that is, $3^{2k} + 7 = 8s$ for some $s \in \mathbb{Z}$. Now for $n = k + 1$ we have

$$3^{2(k+1)} + 7 = 3^{2k+2} + 7 = 3^{2k} \cdot 3^2 + 7$$

$$= 9 \cdot 3^{2k} + 7 \; = 3^{2k} + 8 \cdot 3^{2k} + 7 = (3^{2k} + 7) + 8 \cdot 3^{2k}.$$

The blue bracket on the right is $= 8s$ by the induction hypothesis, so we get $= 8s + 8 \cdot 3^{2k} = 8(s + 3^{2k})$.

The last bracket is $s + 3^{2k} \in \mathbb{Z}$;
so the result is divisible by 8, as required.

$1^\circ\&2^\circ$ by A.M.I. imply that this is true for all $n \in \mathbb{N}$, i.e. $3^{2n} + 7$ is divisible by 8 for all $n \in \mathbb{N}$.

Level of detail

Remark: The solution above is written in every detail.

In other problems simple divisibility properties can be used without such details:

like "if integers a and b are both divisible by integer c,

then $a + b$ is also divisible by c,

and if d is another integer, then ad is also divisible by c".

You had this type of properties in the Algebra module.

Guessing a formula

Induction works when we already guessed the formula.

In the following example we must guess first.

Example

Guess the formula for $1^2 + 2^2 + 3^2 + \cdots + n^2$, and then prove it by induction.

Terms are 'of order' n^2 (may be, 'on average' $n^2/2$? or $n^2/5$? or..?).

We have n terms, and $n \times n^2 = n^3$, so we guess:

$= an^3 + bn^2 + cn + d$, some polynomial of degree 3,

but the coefficients are yet to be determined.

Method of undetermined coefficients

In many parts of mathematics:

Method of undetermined coefficients: when we know the form of the answer, write it with unknown (undetermined) coefficients, and then determine them by using some equations.

Intelligent guess

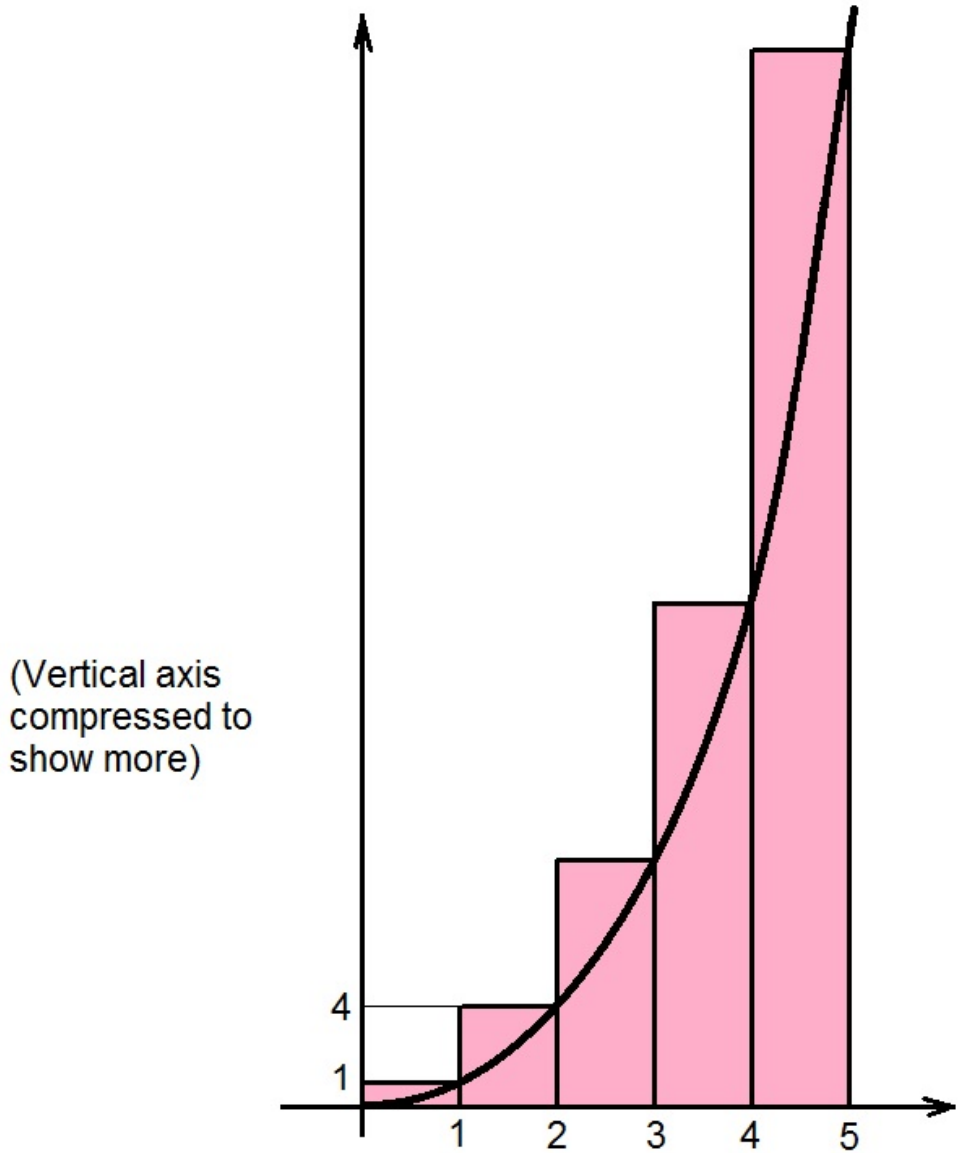
We guess that

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = an^3 + bn^2 + cn + d.$$

But first we simplify our task by making an '*intelligent guess*': we know

$$\int_0^n x^2 dx = x^3/3\Big|_0^n = n^3/3 - 0 = n^3/3.$$

This is the area under the graph $y = x^2$ (over the interval $[0, n]$).



Intelligent guess

Rough approximation of the same area:
the sum of rectangles with base 1 over intervals $[k-1,\ k]$ of height k^2, which have area k^2,

in total $=$ our sum $1^2 + 2^2 + 3^2 + \cdots + n^2$.

Exact area is $\frac{n^3}{3}$, so this rough approximation prompts our *intelligent guess:*

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{3}n^3 + bn^2 + cn + d.$$

Still need to determine b, c, d.

Finding the coefficients

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{3}n^3 + bn^2 + cn + d$$

Substitute $n = 1, 2, 3$: obtain a system of simultaneous equations with unknowns b, c, d:

$$1^2 = 1 = \frac{1}{3}1^3 + b \cdot 1^2 + c \cdot 1 + d = \frac{1}{3} + b + c + d$$

$$1^2 + 2^2 = 5 = \frac{1}{3}2^3 + b \cdot 2^2 + c \cdot 2 + d = \frac{8}{3} + 4b + 2c + d$$

$$1^2 + 2^2 + 3^2 = 14 = \frac{1}{3}3^3 + b \cdot 3^2 + c \cdot 3 + d = 9 + 9b + 3c + d$$

$$1 = 1/3 + b + c + d$$
$$5 = 8/3 + 4b + 2c + d$$
$$14 = 9 + 9b + 3c + d$$

Easy to solve: from 1st eq'n $d = 2/3 - b - c$,
substitute into 2nd: $5 = 8/3 + 4b + 2c + 2/3 - b - c$,
whence $c = 5/3 - 3b$; subst. c and d into 3rd:
$14 = 9 + 9b + 3(5/3 - 3b) + (2/3 - b - (5/3 - 3b))$,
whence $b = 1/2$, then $c = 5/3 - 3/2 = 1/6$ and
$d = 2/3 - 1/2 - 1/6 = 0$.
Thus, $b = 1/2,\ c = 1/6,\ d = 0$, so our guess is

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n.$$

Our guess is

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$$
$$= \frac{2n^3 + 3n^2 + n}{6}.$$

Is it proved?

Yes, if known that the answer must be a polynomial of degree 3 in n.

No, if there is no such a guarantee.

Our guess: $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{2n^3 + 3n^2 + n}{6}$.

We can check more values: say, $n = 5$:

l.h.s.: $1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55$;

r.h.s.: $\dfrac{2.5^3 + 3.5^2 + 5}{6} = \dfrac{250 + 75 + 5}{6} = \dfrac{330}{6} = 55$, the same, OK.

But no matter how many special cases we check, this is not a proof of a general theorem in mathematics!

Proving by induction

So far remains a conjecture, needs to be proved to become a mathematical result.

Example

We **prove by induction** that

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{2n^3 + 3n^2 + n}{6}.$$

1°. For $n = 1$ we have $1^2 = 1 = \frac{2 \cdot 1^3 + 3 \cdot 1^2 + 1}{6} = \frac{6}{6}$, true.

2°. Assume true for $n = k$, that is,

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{2k^3 + 3k^2 + k}{6}.$$

Need to derive for $n = k + 1$

(and we may use the assumption for $n = k$).

L.h.s. for $n = k + 1$ is:

$$1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 =$$

using the induction hypothesis:

$$= \frac{2k^3 + 3k^2 + k}{6} + (k+1)^2$$

$$= \frac{2k^3 + 3k^2 + k + 6k^2 + 12k + 6}{6}$$

$$= \frac{2k^3 + 9k^2 + 13k + 6}{6}.$$

R.h.s. for $n = k + 1$ is

$$\frac{2(k+1)^3 + 3(k+1)^2 + (k+1)}{6}$$

$$= \frac{2k^3 + 6k^2 + 6k + 2 + 3k^2 + 6k + 3 + k + 1}{6}$$

$$= \frac{2k^3 + 9k^2 + 13k + 6}{6},$$

the same: L.h.s=R.h.s., as required.

Now all is proved: 1° and 2° together imply by AMI that the formula is true for all $n \in \mathbb{N}$.

Examples do not prove

Remark: Checking few, even many, first cases is not enough.

Example

Values of $f(n) = n^2 + n + 41$ for $n = 1, 2, 3, \ldots$.

Several first happen to be prime numbers : $f(1) = 43$ prime, $f(2) = 47$ prime, $f(3) = 53$ prime, ...

Actually all 39 first values are primes!

But this value is not always a prime: for $n = 41$ the value is divisible by 41.

(It is also not a prime for $n = 40$; why?)

Induction must be 'based'

Remark: Induction step alone is also not enough.

Example

"Proof" that $2^n > 8n$.
Suppose that true for $n = k$: $2^k > 8k$;
then for $n = k + 1$ we have $2^{k+1} = 2 \times 2^k = 2^k + 2^k$

by the induction hypothesis

$$> 8k + 8k \geq 8k + 8 = 8(k + 1).$$

So the induction step is proved.

But here the base is not true: $2^1 = 2 < 8 \times 1$ and $2^2 = 4 < 8 \times 2$.

However, once we have a base, albeit not for $n = 1$, but further, plus the step proved, we get a correct result: here, for example, base $2^6 = 64 > 8 \times 6 = 48$, plus the step, imply that $2^n > 8n$ for all $n \geq 6$.

Extended A.M.I. (a different starting point).

To prove that a proposition (or property) $P(n)$ is true for all positive integers $n \geq n_0$, it suffices to prove

1°. $P(n_0)$ is true, and

2°. $P(k) \Rightarrow P(k+1)$ for any $k \geq n_0$
(note that step for $k \geq n_0$).

Could be another axiom, but better to keep axioms to a minimum.

This Extended AMI follows from the original AMI.

Theorem

Extended AMI follows from AMI.

Proof. Given a proposition (or property) $P(n)$ for $n \in \mathbb{N}$ such that

$P(n_0)$ is true, and $P(k) \Rightarrow P(k+1)$ for any $k \geq n_0$.

Need to prove that $P(n)$ is true for all $n \geq n_0$.

Define a new proposition $Q(m) = P(m + n_0 - 1)$.

We now prove that $Q(m)$ is true for all $m \in \mathbb{N}$

by induction on m.

1°. For $m = 1$ we have $Q(1) = P(1 - n_0 - 1) = P(n_0)$, is true by hypothesis.

2°. Assume that $Q(s) = P(s + n_0 - 1)$ is true.

Here $k = s + n_0 - 1 \geq n_0$, so by hypothesis
$P(k + 1) = P(s + n_0 - 1 + 1)$ is also true,

which is the same as $Q(s + 1)$.

Thus, we proved that
$Q(s)$ true $\Rightarrow$ $Q(s + 1)$ true.

By the original AMI,
1° and 2° imply that $Q(m) = P(m + n_0 - 1)$ is true for all $m \in \mathbb{N}$.

But this means that $P(n)$ is true for all $n \geq n_0$. $\square$

Example

Prove that $n^2 \leq 2^n$ for all $n \geq 4$.

(Note: not true for all $n \in \mathbb{N}$, as $3^2 \not\leq 2^3$.)

EAMI: 1°. For $n = 4$ we have $4^2 = 16 \leq 16 = 2^4$, true.

2°. Assume that $k^2 \leq 2^k$ (and that $k \geq 4$).

Need $(k+1)^2 \leq 2^{k+1}$.

R.h.s.: $2^{k+1} = 2 \cdot 2^k = 2^k + 2^k \geq k^2 + k^2 = 2k^2$ by the induction hypothesis.

L.h.s. is $(k+1)^2 = k^2 + 2k + 1$.

If we had $2k^2 \geq k^2 + 2k + 1$, then all is proved;

so we need $k^2 \geq 2k + 1$.

.... we need $k^2 \geq 2k + 1$.

One way is solving inequality by finding roots, etc., and using $k \geq 4$.

Perhaps simpler: $k^2 \geq 4k$ since $k \geq 4$,

and $4k = 2k + 2k \geq 2k + 2 \geq 2k + 1$.

This finishes proof of 2°.

Now 1° and 2° by EAMI imply that the inequality is true for all $n \geq 4$.

Binomial coefficients

Definition.

Binomial coefficient $\binom{n}{k}$
(often read as "n choose k",
in fact meaning "choose k out of n") is

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

This includes values

$$\binom{n}{0} = 1 \qquad \text{and} \qquad \binom{n}{n} = 1.$$

Combinatorial Fact.

$\binom{n}{k}$ is the number of ways of choosing k elements out of n different elements (irrespective of order).

Proof: Indeed, the first can be chosen in n ways,

the second in $n-1$ ways (among the remaining $n-1$),

third in $n-2$ ways, and so on,

altogether $n(n-1)(n-2)\cdots(n-k+1)$ ways.

But this was in a particular order, so each unordered choice counted several times. Namely, there are $k!$ ways to rearrange k elements in different orders (this follows from the same argument: the first is chosen in k ways, second in $k-1$ ways, and so on).

Thus, we must divide the number

$$n(n-1)(n-2)\cdots(n-k+1)$$

of ordered choices of k out of n by $k!$,

which results in exactly the r.h.s. of the formula above:

$$\frac{n(n-1)(n-2)\cdots(n-k+1)}{1\cdot 2\cdot 3\cdots k} = \frac{n!}{k!(n-k)!}.$$

Property:

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

Proof: Can be proved by induction.

Easier to use the Combinatorial Fact:

Choose one fixed element out of those n. Then

$\binom{n-1}{k-1}$ is the number of choices

of $k-1$ elements out of $n-1$ remaining elements,

that is, the number of choices of k elements that **include** the fixed one.

The number of choices of k elements

that **do not include** the fixed one is

$\binom{n-1}{k}$ because we choose k out of $n-1$

(without the fixed one).

Together we have all possible choices of k elements,

both including the fixed one and not including it.

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

Example

For any $n \in \mathbb{N}$,

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

Induction on n:

1°. For $n = 1$: $\binom{1}{0} + \binom{1}{1} = 1 + 1 = 2^1$, true.

2°. Suppose formula is true for $n = k$. Consider $n = k + 1$: need

$$\binom{k+1}{0} + \binom{k+1}{1} + \binom{k+1}{2} + \cdots$$

$$\cdots + \binom{k+1}{k+1-1} + \binom{k+1}{k+1} = 2^{k+1}.$$

On the left, use Property above for every term:

$$\binom{k+1}{i} = \binom{k}{i-1} + \binom{k}{i} \text{ and substitute:}$$

$$1 + \left[\binom{k}{0} + \binom{k}{1}\right] + \left[\binom{k}{1} + \binom{k}{2}\right] + \left[\binom{k}{2} + \binom{k}{3}\right] + \cdots$$

$$\cdots + \left[\binom{k}{k-1} + \binom{k}{k}\right] + 1$$

(we also replaced first and last terms by 1).

Now re-arrange brackets, using also first and last terms as $1 = \binom{k}{0}$ and $1 = \binom{k}{k}$:

$$\left[\binom{k}{0} + \binom{k}{0}\right] + \left[\binom{k}{1} + \binom{k}{1}\right] + \left[\binom{k}{2} + \binom{k}{2}\right] + \cdots$$

$$\cdots + \left[\binom{k}{k-1} + \binom{k}{k-1}\right] + \left[\binom{k}{k} + \binom{k}{k}\right].$$

We now see that each bracket is double the term from the sum for $n = k$: l.h.s. is therefore

$$2 \cdot \left[\binom{k}{0} + \binom{k}{1} + \binom{k}{2} + \cdots + \binom{k}{k-1} + \binom{k}{k}\right].$$

Use the induction hypothesis and replace the big bracket by 2^k. The result is $2 \cdot 2^k = 2^{k+1}$, as required. Step is proved.

Now 1° and 2° by AMI imply that the formula is true for all $n \in \mathbb{N}$.

Example ("Fermat's Little Theorem.")

Let p be a prime number. Then $n^p - n$ is divisible by p for any $n \in \mathbb{N}$.

(You may have had this in Algebra.) Now as an exercise in math. induction.

1°. For $n = 1$: $\quad 1^p - 1 = 0 = p \cdot 0$ is divisible by p.

2°. Assume that $k^p - k$ is divisible by p. Consider $(k+1)^p - (k+1)$: by the binomial formula

$$= k^p + \binom{p}{1} k^{p-1} \cdot 1^1 + \binom{p}{2} k^{p-2} \cdot 1^2 + \cdots$$

$$\cdots + \binom{p}{p-2} k^2 \cdot 1^{p-2} + \binom{p}{p-1} k^1 \cdot 1^{p-1} + 1 - k - 1 =$$

(canceling $+1$ and -1 out and rearranging):

$$= k^p - k + \binom{p}{1} k^{p-1} + \binom{p}{2} k^{p-2} + \cdots$$

$$\cdots + \binom{p}{p-2} k^2 + \binom{p}{p-1} k^1.$$

By the induction hypothesis, $k^p - k$ is divisible by p,

It remains to prove that all other terms are divisible by p.

For any $1 \leq j \leq p-1$ the binomial coefficient $\binom{p}{j} = \frac{p!}{j!(p-j)!}$ is divisible by p.

It is a positive integer, since $=$ the number of choices of j objects of p.

Hence all the prime-powers in the denominator must occur in the numerator and vanish when the fraction is reduced. But the numerator has the prime factor p, which does not occur in the denominator, since $j < p$ and $p - j < p$. Therefore the factor p **must remain** in the reduced fraction, which is an integer; hence this integer is divisible by p. Thus, all terms are integers divisible by p.

So we proved induction step.

1°& 2° by AMI imply that the assertion is true for all $n \in \mathbb{N}$.

Higher derivatives

n-th derivative of $f(x)$ is denoted by $f^{(n)}(x)$.

Just taking derivative n times.

In particular, $f^{(1)} = f'$; $f^{(2)} = f'' = (f')'$; and so on.

We know: $(f+g)' = f' + g'$; then
$(f+g)'' = (f'+g')' = f'' + g''$,

and so on: $(f+g)^{(n)} = f^{(n)} + g^{(n)}$ "sum rule".

Product rule: $(f \cdot g)' = f' \cdot g + f \cdot g'$.

Formula for $(f \cdot g)^{(n)}$?

Example (The Leibnitz Formula)

For functions $u = u(x)$ and $v = v(x)$,

$$(u \cdot v)^{(n)} = u^{(n)}v + \binom{n}{1} u^{(n-1)}v^{(1)} + \binom{n}{2} u^{(n-2)}v^{(2)} + \cdots$$

$$\cdots + \binom{n}{n-1} u^{(1)}v^{(n-1)} + uv^{(n)}.$$

Proof: Induction on n.

1°. For $n = 1$ we have $(uv)^{(1)} = u^{(1)}v + uv^{(1)}$, the product rule.

2°. Assume formula true for $n = k$;
consider for $n = k + 1$:

$$(uv)^{(k+1)} = ((uv)^{(1)})^{(k)}$$

$$= (u^{(1)}v + uv^{(1)})^{(k)} \text{ by the product rule,}$$

$$= (u^{(1)}v)^{(k)} + (uv^{(1)})^{(k)} \quad \text{by the sum rule.}$$

Apply the induction hypothesis to each summand
(using $(f^{(1)})^{(j)} = f^{(j+1)}$), in two rows:

$$u^{(k+1)}v + \binom{k}{1}u^{(k)}v^{(1)} + \binom{k}{2}u^{(k-1)}v^{(2)} + \cdots \quad + \binom{k}{r}u^{(k+1-r)}v^{(r)} + \cdot$$

$$+ u^{(k)}v^{(1)} + \binom{k}{1}u^{(k-1)}v^{(2)} + \cdots + \binom{k}{r-1}u^{(k+1-r)}v^{(r)} +$$

(the same)

$$u^{(k+1)}v + \binom{k}{1}u^{(k)}v^{(1)} + \binom{k}{2}u^{(k-1)}v^{(2)} + \cdots \quad + \binom{k}{r}u^{(k+1-r)}v^{(r)} + \cdot$$

$$+ u^{(k)}v^{(1)} + \binom{k}{1}u^{(k-1)}v^{(2)} + \cdots + \binom{k}{r-1}u^{(k+1-r)}v^{(r)} +$$

Sums aligned so the same derivatives are one under another. Collect terms:

$$u^{(k+1)}v + \left[\binom{k}{1} + 1\right]u^{(k)}v^{(1)} + \cdots$$

$$\cdots + \left[\binom{k}{r} + \binom{k}{r-1}\right]u^{(k+1-r)}v^{(r)} + \cdots + uv^{(k+1)}.$$

Apply Property $\binom{k}{r} + \binom{k}{r-1} = \binom{k+1}{r}$ to each bracket (using also $1 = \binom{k}{0} = \binom{k}{k}$):

$$u^{(k+1)}v + \binom{k+1}{1} u^{(k+1-1)}v^{(1)} + \dots$$

$$\dots + \binom{k+1}{r} u^{(k+1-r)}v^{(r)} + \dots + \binom{k+1}{k} u^{(1)}v^{(k)} + uv^{(k+1)},$$

as required for $n = k + 1$.

1°& 2° by A.M.I. imply that the formula is true for all $n \in \mathbb{N}$.

Example

Differentiate $(x^2 \sin x)^{(4)}$. By the Leibnitz formula

$$= (x^2)^{(4)} \sin x + \binom{4}{1}(x^2)^{(3)}(\sin x)^{(1)} + \binom{4}{2}(x^2)^{(2)}(\sin x)^{(2)} + \binom{4}{1}(x^2)^{(1)}(\sin x)^{(3)} + x^2(\sin x)^{(4)}.$$

We have $(x^2)^{(1)} = 2x$, $(x^2)^{(2)} = (2x)' = 2$;

$(x^2)^{(3)} = 2' = 0$,

and $(\sin)' = \cos$, $(\cos)' = -\sin$, etc.

So $\cdots = 0 + 0 + 6 \cdot 2(-\sin x) + 4 \cdot 2x(-\cos x) + x^2 \sin x$

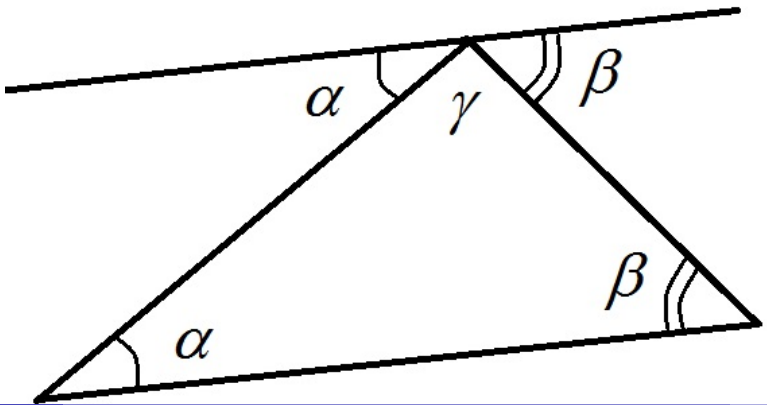
$= (x^2 - 12)\sin x - 8x \cos x.$

Induction in geometry

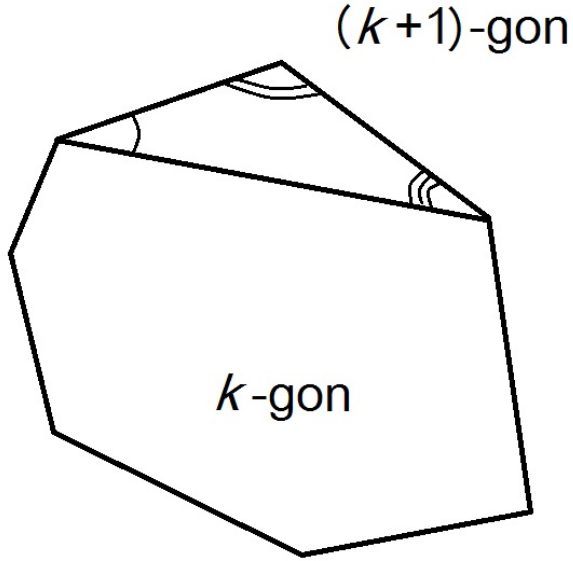
Example (The sum of angles)

The sum of angles in any convex n-gon (figure with n straight sides), $n \geq 3$, is equal to $(n-2)\pi$ in radians, $= (n-2) \cdot 180^\circ$.

Proof: 1°. The base is $n = 3$. For a triangle, the sum of angles is $180^\circ = (3-2) \cdot 180^\circ$.
Proved in geometry: draw parallel line



2°. Suppose this is true for any k-gon. Consider an arbitrary $(k+1)$-gon. We can cut off a triangle:



The remaining k-gon has sum of angles $(k-2)\cdot 180^\circ$ by the induction hypothesis. The angles of the triangle add 180° more. Together the sum of all angles of our $(k+1)$-gon is then $(k-2)\cdot 180^\circ + 180^\circ = (k-1)\cdot 180^\circ = ((k+1)-2)\cdot 180^\circ$, as required.

1°& 2° by EAMI $\Rightarrow$ true for all $n \geq 3$.

Usually induction is easier for equations. Now more examples with inequalities.

Example (Bernoulli's inequality)

If $x > -1$, then $(1+x)^n \geq 1 + nx$
for any positive integer n.

Note that for $x > 0$ the inequality is obvious from the binomial formula:

$$\begin{aligned}(1+x)^n &= 1 + \binom{n}{1}x + \binom{n}{2}x^2 + \binom{n}{3}x^3 + \cdots \\ &= 1 + nx + \text{ all other terms are positive} \\ &\geq 1 + nx.\end{aligned}$$

But this does not work for $-1 < x < 0$.

Proof: $(1+x)^n \geq 1+nx$ if $x > -1$

1°. For $n = 1$: $\quad (1+x)^1 \geq 1 + 1 \cdot x$, true.

2°. Assume true for $n = k$: $\quad (1+x)^k \geq 1 + kx$.

Multiply both parts by $1 + x$
(so l.h.s. becomes l.h.s for $n = k + 1$)
inequality remains valid, since $1 + x > 0$:
$(1+x)^k \cdot (1+x) \geq (1+kx) \cdot (1+x)$;

$$(1+x)^{k+1} \geq 1 + kx + x + kx^2 = 1 + (k+1)x + kx^2.$$

$$\geq 1 + (k+1)x, \text{ since } kx^2 \geq 0.$$

Thus, $(1+x)^{k+1} \geq 1 + (k+1)x$, as required for $n = k + 1$. Step proved.

1°& 2° by AMI $\Rightarrow$ holds for all $n \in \mathbb{N}$.

Example

$n^3 < 3^n$ for all positive integers $n \geq 4$.

1°. For $n = 4$: $\quad 4^3 = 64 < 81 = 3^4$, true.

2°. Assume true for $n = k$ and $k \geq 4$.

For $n = k + 1$ need $(k + 1)^3 < 3^{k+1}$.

By ind. hyp. $k^3 < 3^k$, so $3k^3 < 3^{k+1}$.

So if we prove that $(k + 1)^3 \leq 3k^3$,
then all will be proved.

Need $k^3 + 3k^2 + 3k + 1 \leq 3k^3 = k^3 + k^3 + k^3$.

Clearly, $k^3 \leq k^3$ and $3k^2 \leq k^3$, since $k \geq 4$.

It remains to show that $3k + 1 \leq k^3$.

...It remains to show that $3k + 1 \leq k^3$.

We have $3k + 1 \leq 3k + k = 4k \leq k^3$, since $k \geq 4$. Step proved.

1°& 2° by EAMI imply true for all $n \geq 4$.

'Non-example'

Remark: Not all is easily proved by induction.

Clearly, $1 - 1/n < 1$.

But try proving by induction:

1° fine: $1 - 1/1 = 0 < 1$, true.

2°. Suppose $1 - 1/k < 1$. For $n = k + 1$ we have l.h.s. $1 - 1/(k + 1)$;

trying to use ind. hyp.: $= 1 - 1/k + (1/k - 1/(k + 1))$,

we know that $1 - 1/k < 1$ by ind. hyp.,

but the additional term $(1/k - 1/(k + 1))$ is positive, "makes it worse", so we cannot proceed.

Cumulative induction

In induction step, we may assume not just $P(k)$ is true but even all $P(1), P(2), \ldots, P(k)$ to be true.

Cumulative Axiom of Mathematical Induction.

Suppose that

1° $P(1)$ is true, and

2° if $P(i)$ is true for all $i = 1, 2, \ldots, k$,

then $P(k+1)$ is true;

in other words: $P(1) \& P(2) \& \ldots \& P(k) \Rightarrow P(k+1)$.

Then $P(n)$ is true for all positive integers $n \in \mathbb{N}$.

C.A.M.I. Also can start from some $n = n_0$, E.C.A.M.I.

Example (Prime Factorization Theorem)

Every positive integer $n \geq 2$

is a product of prime numbers.

Cumulative induction on n.

1°. 2 is a prime, OK.

2°. Assume that all positive integers $\leq k$ (and ≥ 2) are products of primes. Need to prove that $k+1$ is a product of primes.

If $k+1$ is a prime, we are done.

If $k+1$ is not a prime, then $k+1 = ab$ where $a, b \in \mathbb{N}$ are smaller than $k+1$ and greater than 1.

By the induction hypothesis both a and b are products of primes: $a = p_1 \cdots p_s$ and $b = q_1 \cdots q_t$ (not necessarily different).

Substitute $k+1 = ab = p_1 \cdots p_s \cdot q_1 \cdots q_t$ – required decomposition for $k+1$.

1°&2° by E.C.A.M.I. imply that all positive integers ≥ 2 are products of primes.

Theorem

C. A. M. I. follows from the ordinary A. M. I.

Proof: Have a proposition $P(n)$ such that

1°. $P(1)$ is true, and

2°. $P(1)\&P(2)\&\ldots\&P(k) \Rightarrow P(k+1)$ for any k.

Need to prove that then $P(n)$ is true for all $n \in \mathbb{N}$.

Form a new proposition $Q(n) = P(1)\&P(2)\&\ldots\&P(n)$.

Prove that $Q(n)$ is true for all $n \in \mathbb{N}$.

1°. $Q(1) = P(1)$ is true by hypothesis.

2°. If $Q(k)$ is true, then

$= P(1)\&P(2)\&\ldots\&P(k)$ is true.

Then $P(k+1)$ is true by hypothesis.

But then all $P(1)$, $P(2)$, $\ldots P(k)$, $P(k+1)$ are true,

which means that $Q(k+1)$ is true.

Step proved in induction for $Q(n)$.

By ordinary AMI,

1° and 2° imply that $Q(n)$ is true for all $n \in \mathbb{N}$.

But $Q(n)$ includes $P(n)$, so $P(n)$ is true for all $n \in \mathbb{N}$.

Recursive definitions

(definitions by mathematical induction)

Sequences (often of numbers): $a_1, a_2, a_3, \ldots,$

with indices $1, 2, 3, \ldots \in \mathbb{N}$.

Short notation: $(a_i)_{i \in \mathbb{N}}$.

(In some books, other notation: $\{a_i\}_{i \in \mathbb{N}}$, etc.)

Some given by a formula, like $a_i = 2^i$,

so it is $2,\ 4,\ 8, \ldots, 2^i, \ldots$.

Recursive Definition Axiom

For a sequence $(a_i)_{i \in \mathbb{N}}$, suppose that

- a_1 is defined, and
- whenever a_k is defined, then a_{k+1} is also defined

  by some rule mathematically

  as $a_{k+1} = f_k(a_k)$ for some functions f_k.

Then a_n is defined for all $n \in \mathbb{N}$.

When proving something about a recursively defined sequence, it is natural to use mathematical induction.

Example

Let $a_1 = 1$ and $a_{k+1} = (k+1)a_k$.

Then $a_n = n!$ for all $n \in \mathbb{N}$.

Proof:

1°. $a_1 = 1 = 1!$, true.

2°. Suppose $a_k = k!$.

Then $a_{k+1} = (k+1)a_k$ by the definition;

substitute by induction hypothesis:

$= (k+1)k! = (k+1)!$, as required.

By AMI 1° and 2° imply that $a_n = n!$ for all $n \in \mathbb{N}$.

Example

Let $a_1 = 5$ and $a_n = 3a_{n-1} + 2$.

Prove that then $a_n = 2 \cdot 3^n - 1$ for all $n \in \mathbb{N}$.

1°. $a_1 = 5 = 2 \cdot 3^1 - 1 = 6 - 1$, true.

2°. Suppose $a_k = 2 \cdot 3^k - 1$.

By the definition: $a_{k+1} = 3a_k + 2$

Substitute by the induction hypothesis:

$$= 3(2 \cdot 3^k - 1) + 2 = 2 \cdot 3 \cdot 3^k - 3 + 2$$

$$= 2 \cdot 3^{k+1} - 1,$$

as required for $n = k + 1$.

By AMI, 1° & 2° $\Rightarrow$ $a_n = 2 \cdot 3^n - 1$ for all $n \in \mathbb{N}$.

Cumulative Recursive Definition

Cumulative Recursive Definition Axiom

For a sequence $(a_i)_{i \in \mathbb{N}}$, suppose that

- a_1 is defined, and
- when $a_1, a_2, \ldots, a_k$ are defined,

  then a_{k+1} is also defined

  (as $a_{k+1} = f_k(a_1, \ldots, a_k)$ for some function f_k).

Then a_n is defined for all $n \in \mathbb{N}$.

Naturally, if defined by cumulative recursion

$\Rightarrow$ use cumulative induction for proving.

Example

Let $a_1 = 1, \quad a_2 = 1,$

and $a_{k+1} = a_1 + a_2 + \cdots + a_k$ for all $k \geq 3.$

Prove that $a_n = 2^{n-2}$ for all $n \geq 2.$

Proof:

$1^\circ.$ $a_2 = 1 = 2^{2-2} = 2^0,$ true.

2°. Suppose $a_2 = 2^0,\ a_3 = 2^1, \ldots, a_k = 2^{k-2}$.

By the definition $a_{k+1} = a_1 + a_2 + \cdots + a_k$

Substitute by the induction hypothesis:

$$= 1 + 1 + 2 + 4 + \cdots + 2^{k-2}$$

by formula for geometric series:

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

$= 1 + 2^{k-1} - 1 = 2^{(k+1)-2}$, as required.

By Cumulative A.M.I.,

1° and 2° imply that $a_n = 2^{n-2}$ for all $n \geq 2$.

Often not all previous terms are needed. But no harm in assuming that ind. hyp. is true for all previous terms.

Example

Let $a_1 = 0, \quad a_2 = 6,$

and $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geq 3.$

Prove that $a_n = 2 \cdot 3^n - 3 \cdot 2^n$ for all $n \in \mathbb{N}.$

Proof:

1°. Recursive formula works only from $n = 3,$

so need to check the base for $n = 1$ and $n = 2$:

$a_1 = 0 = 2 \cdot 3^1 - 3 \cdot 2^1 = 6 - 6,$ true.

$a_2 = 6 = 2 \cdot 3^2 - 3 \cdot 2^2 = 18 - 12,$ true.

2°. Suppose $a_n = 2 \cdot 3^n - 3 \cdot 2^n$ for all $n \leq k$.

By def.: $a_{k+1} = 5a_k - 6a_{k-1}$.

Substitute by the induction hypothesis:

$$= 5(2 \cdot 3^k - 3 \cdot 2^k) - 6(2 \cdot 3^{k-1} - 3 \cdot 2^{k-1})$$

$$= 10 \cdot 3^k - 15 \cdot 2^k - 12 \cdot 3^{k-1} + 18 \cdot 2^{k-1} =$$

(arranging 3^{k-1} and 2^{k-1} for collecting terms:)

$$= 30 \cdot 3^{k-1} - 30 \cdot 2^{k-1} - 12 \cdot 3^{k-1} + 18 \cdot 2^{k-1}$$

$$= (30 - 12) \cdot 3^{k-1} + (-30 + 18) \cdot 2^{k-1}$$

$$= 18 \cdot 3^{k-1} - 12 \cdot 2^{k-1}$$

$$= 2 \cdot 3^{k+1} - 3 \cdot 2^{k+1}, \text{ as required.}$$

By C.A.M.I., 1° and $2^\circ \Rightarrow a_n = 2 \cdot 3^n - 3 \cdot 2^n \ \forall n \in \mathbb{N}$.

Fibonacci numbers

Definition: Fibonacci numbers

... are defined as $F_1 = 1$, $F_2 = 1$,

and $F_n = F_{n-2} + F_{n-1}$ for $n \geq 3$.

1, 1, 2, 3, 5, 8, 13, 21, ...

Have many nice properties,

appear in various maths problems,

even in nature:-).

Example

Let $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-2} + F_{n-1}$ for $n \geq 3$ (Fibonacci numbers).

Prove that $F_{2n} = F_1 + F_3 + \cdots + F_{2n-1}$ for every $n \in \mathbb{N}$.

Proof: 1°. For $n = 1$: $F_2 = 1 = F_1$, true.

2°. Suppose $F_{2k} = F_1 + F_3 + \cdots + F_{2k-1}$.

Next $F_{2(k+1)} = F_{2k+2}$ by definition $= F_{2k} + F_{2k+1}$

(can apply the definition, since $2k + 2 \geq 4 \geq 3$).

Use the induction hypothesis and substitute:

$= F_1 + F_3 + \cdots + F_{2k-1} + F_{2k+1}$ — as required.

By A.M.I. 1° and 2° $\Rightarrow$ true $\forall n \in \mathbb{N}$.

Recap of Ch. 1. Math. Induction:

Math. induction: basis ($P(1)$ true)

$+$ step ($P(k)$ true $\Rightarrow$ $P(k+1)$ true),

then $P(n)$ true for all $n \in \mathbb{N}$.

Extended: start from $n = n_0$ (rather than from $n = 1$).

Cumulative: basis $+$ step $P(n)$ true for all $n \leq k$

(not just for $n = k$) $\Rightarrow$ $P(k+1)$ true;

then $P(n)$ true for all $n \in \mathbb{N}$.

Recursive definitions by induction — proofs by induction.