Math 235 Fall 2024, Lecture 1 stenogram: Induction and modular arithmetic

website: `https://www.cip.ifi.lmu.de/~grinberg/t/24f`

0.1. What is this about?

My name is Darij Grinberg.

See the above website for things you need to know about this class, for the notes and for the homework.

This is a course on **mathematical problem-solving**, i.e., proving theorems, finding formulas, finding counterexamples, answering questions, etc. – but unlike most courses, this will be a creative activity, since it won't be clear right away how to proceed.

1. Induction

I assume that you all know (mathematical) induction, and now want to focus on places where it can be used.

Here is an example where this is fairly clear:

> **Exercise 1.** Prove that every integer $n \geq 0$ satisfies
>
> $$\underbrace{\frac{1}{1} - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{2n-1} - \frac{1}{2n}}_{= \sum_{i=1}^{2n} \frac{(-1)^{i-1}}{i}} = \underbrace{\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n}}_{= \sum_{i=1}^{n} \frac{1}{n+i} = \sum_{i=n+1}^{2n} \frac{1}{i}}.$$

Solution. Induct on n.

Base case: For $n = 0$, the claim is just $0 = 0$ (since an empty sum is 0 by definition).

Induction step: Let n be a positive integer. Assume (as the induction hypothesis) that the claim holds for $n - 1$ instead of n.

$$\frac{1}{1} - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{2n-3} - \frac{1}{2n-2}$$
$$= \frac{1}{n} + \frac{1}{n+1} + \cdots + \frac{1}{2n-2}.$$

Now we must prove that the claim also holds for n. In other words, we must prove

$$\frac{1}{1} - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{2n-1} - \frac{1}{2n} = \frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n}.$$

The LHS here is

$$\begin{aligned}
&\frac{1}{1}-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots+\frac{1}{2n-1}-\frac{1}{2n} \\
&=\underbrace{\frac{1}{1}-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots+\frac{1}{2n-3}-\frac{1}{2n-2}}_{\text{the old LHS}}+\frac{1}{2n-1}-\frac{1}{2n},
\end{aligned}$$

while the RHS here is

$$\begin{aligned}
&\frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{2n} \\
&=\underbrace{\frac{1}{n}+\frac{1}{n+1}+\cdots+\frac{1}{2n-2}}_{\text{the old RHS}}+\frac{1}{2n-1}+\frac{1}{2n}-\frac{1}{n}.
\end{aligned}$$

So, in order to prove that the new LHS equals the new RHS, we must only show that the new addends are equal, i.e., that

$$\frac{1}{2n-1}-\frac{1}{2n}=\frac{1}{2n-1}+\frac{1}{2n}-\frac{1}{n}.$$

This can be proved straightforwardly by bringing the fractions to a common denominator. Or we can cancel the first fractions and easily deal with the rest. So the induction step is complete, and the exercise is solved. ■

Comments:

1. This was an example of an induction proof that is completely straightforward. The reason is that the LHS and the RHS change very predictably when you go from $n-1$ to n.

Here is an example of a non-straightforward induction proof.

> **Exercise 2.** Fix a positive integer n. An n**-bitstring** shall mean an n-tuple $(a_1, a_2, \ldots, a_n) \in \{0,1\}^n$ of bits. (Recall that a **bit** is an element of $\{0,1\}$.)
>
> Two n-bitstrings $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ **differ in exactly one bit** if there is exactly one $i \in \{1,2,\ldots,n\}$ such that $a_i \neq b_i$. For instance, $(0,1,1,0)$ differs from $(0,0,1,0)$ in exactly one bit.
>
> Prove that we can arrange all the 2^n many n-bitstrings in a cyclic list $(b_1, b_2, \ldots, b_{2^n})$ such that for each $i \in \{1,2,\ldots,2^n\}$, the two bitstrings b_i and b_{i-1} differ in exactly one bit, where $b_0 = b_{2^n}$.

Solution. We try to induct on n.

Base case: For $n = 1$, we just list the two 1-bitstrings in the obvious order: (0, 1). (Here, 0 and 1 really mean the 1-bitstrings (0) and (1); we are not writing the parentheses and the commas.)

Induction step: Let $n > 1$. Assume (as the IH = induction hypothesis) that there is such an arrangement for $n-1$ instead of n. That is, we can arrange all the 2^{n-1} many $(n-1)$-bitstrings in a cyclic list

$$(b_1, b_2, \ldots, b_{2^{n-1}})$$

in a good way (i.e., such that each b_i differs from b_{i-1} in exactly one bit, and b_1 differs from $b_{2^{n-1}}$ in exactly one bit). Now let us try to arrange the 2^n many n-bitstrings in a similar way.

The 2^n many n-bitstrings are

$$0b_1,\ 0b_2,\ \ldots,\ 0b_{2^{n-1}},\ 1b_1,\ 1b_2,\ \ldots,\ 1b_{2^{n-1}}.$$

Then we list them as follows:

$$0b_1,\ 0b_2,\ \ldots,\ 0b_{2^{n-1}},\ 1b_{2^{n-1}},\ \ldots,\ 1b_2,\ 1b_1.$$

This is a good arrangement, so the induction step is complete and we are done.

Comments:

1. This kind of arrangement is called a **Gray code**.
2. There are similar constructions for n-tuples of elements of other sets than $\{0, 1\}$.
3. More generally, such arrangements are particular cases of **Hamiltonian cycles in graphs**.

1.1. Fibonacci numbers I

Definition 1.1.1. The **Fibonacci sequence** is the sequence $(f_0, f_1, f_2, \ldots)$ of nonnegative integers defined recursively by

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

The entries of this sequence are called the **Fibonacci numbers**.

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

Exercise 3. Prove that each integer $n \geq 0$ satisfies

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

Solution. Induction on n.
Base case: For $n = 0$, this is saying that $0 = f_2 - 1$, which is indeed true.
Induction step: Going from n to $n+1$, we have

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

qed. ■

Exercise 4. Prove that for every positive integer n, we have

$$f_{n+1} f_{n-1} - f_n^2 = (-1)^n .$$

Solution. Induction on n.
Base case: $n = 1$, straightforward.
Induction step: Let's go from n to $n+1$. So the IH says that $f_{n+1} f_{n-1} - f_n^2 = (-1)^n$, and our goal is to prove that $f_{n+2} f_n - f_{n+1}^2 = (-1)^{n+1}$.
We have

$$\begin{aligned} \underbrace{f_{n+2}}_{\substack{= f_{n+1} + f_n \\ \text{(by the definition} \\ \text{of the Fibonacci seq)}}} f_n - f_{n+1}^2 &= (f_{n+1} + f_n) f_n - f_{n+1}^2 \\ &= f_{n+1} f_n + \underbrace{f_n^2}_{\substack{= f_{n+1} f_{n-1} - (-1)^n \\ \text{(by our IH)}}} - f_{n+1}^2 \\ &= f_{n+1} f_n + f_{n+1} f_{n-1} - (-1)^n - f_{n+1}^2 \\ &= f_{n+1} \underbrace{(f_n + f_{n-1} - f_{n+1})}_{\substack{= 0 \\ \text{(since } f_{n+1} = f_n + f_{n-1})}} - (-1)^n \\ &= -(-1)^n = (-1)^{n+1}, \end{aligned}$$

qed. ■

Exercise 5 (addition formula for Fibonacci numbers)**.** Prove that for any integers $n, m \geq 0$, we have

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

Solution. Induct on n. (We could just as well induct on m, but this would not make any difference, since the roles are symmetric.)

Base case: For $n = 0$, this is saying $f_{m+1} = \underbrace{f_0}_{=0} f_m + \underbrace{f_1}_{=1} f_{m+1}$.

Induction step: Let's go from $n-1$ to n. So let n be a positive integer. Assume as the IH that the claim holds for $n-1$ instead of n. In other words, we assume that

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

Our goal is to prove that the claim also holds for n, i.e., to prove that

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

So let $m \geq 0$. Then,

$$\begin{aligned}
f_{n+m+1} &= \underbrace{f_{n+m}}_{\substack{= f_{n-1} f_m + f_n f_{m+1} \\ \text{(by the IH)}}} + \underbrace{f_{n+m-1}}_{\substack{= f_{n-1} f_{m-1} + f_n f_m \\ \text{(by the IH, applied to } m-1 \text{ instead of } m)}} \\
&= f_{n-1} f_m + f_n f_{m+1} + f_{n-1} f_{m-1} + f_n f_m \\
&= f_{n-1} f_m + f_{n-1} f_{m-1} + f_n f_{m+1} + f_n f_m \\
&= f_{n-1} \underbrace{(f_m + f_{m-1})}_{= f_{m+1}} + f_n f_{m+1} + f_n f_m \\
&= f_{n-1} f_{m+1} + f_n f_{m+1} + f_n f_m = \underbrace{(f_{n-1} + f_n)}_{= f_{n+1}} f_{m+1} + f_n f_m \\
&= f_{n+1} f_{m+1} + f_n f_m = f_n f_m + f_{n+1} f_{m+1}.
\end{aligned}$$

There is one little catch: Applying the IH to $m-1$ instead of m was only allowed when $m - 1 \geq 0$. So we need to consider the $m = 0$ case separately. But this case is easy anyway (just like the $n = 0$ case), so the induction step is complete both for positive and for zero m. ■

Exercise 6. Prove **Binet's formula** for the Fibonacci numbers:

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

for all $n \geq 0$, where we set

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

(Note that φ is known as the **golden ratio**; φ and ψ are the two roots of the quadratic equation $x^2 = x + 1$.)

Solution. Induction on n:
Base case: Easy for $n = 0$.
Induction step: Let's try to go from n to $n + 1$. So our IH is

$$f_n = \frac{1}{\sqrt{5}}\varphi^n - \frac{1}{\sqrt{5}}\psi^n,$$

and our goal is to show that

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

We try to do this:

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

But what is f_{n-1} ? Our IH doesn't tell us anything about it.

So this particular kind of induction doesn't work here.

The way to proceed is something known as **strong induction**: an induction principle where instead of going from $n - 1$ to n, you go from $0, 1, \ldots, n - 1$ together to n. So the IH is not just saying "the claim is true for $n - 1$", but actually is saying "the claim is true for all numbers up to $n - 1$ (inclusive)". In particular, if you are using this principle, you can use the IH not just for $n - 1$ but also for $n - 2$.