Math 235 Fall 2024, Lecture 2 stenogram: Induction and modular arithmetic cont'd

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

Planning:

- **Recitation:** Fri 12M–1PM usually [Korman Center, the common room, next to 245; otherwise, Korman 263], Mon 12M–1PM next week.
- **Office hours:** Wed 12M–1PM.
- **Bug bounty:** +1 homework point per nontrivial correction to the text or the exercises, up to 25 points over the quarter.

  [Jonathan Parlett, Sofie Tauris got their first point.]

1. Induction (cont'd)

Last time, we saw a few induction proofs:

Exercise 1. Prove that every integer $n \geq 0$ satisfies

$$\underbrace{\frac{1}{1} - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} \pm \cdots + \frac{1}{2n-1} - \frac{1}{2n}}_{= \sum_{i=1}^{2n} \frac{(-1)^{i-1}}{i}} = \underbrace{\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n}}_{= \sum_{i=1}^{n} \frac{1}{n+i} = \sum_{i=n+1}^{2n} \frac{1}{i}}.$$

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 $b_0 = b_{2^n}$.

Definition 1.0.1. 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

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

Exercise 4 (Cassini identity)**.** Prove that for every positive integer n, we have

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

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

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

Let's continue with induction.

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 $n-2$.

The strong induction principle is saying that if you want to prove a statement $\mathcal{A}(n)$ for all integers $n \geq 0$, it suffices to show that for each $n \geq 0$, the implication

$$(\mathcal{A}(0) \wedge \mathcal{A}(1) \wedge \cdots \wedge \mathcal{A}(n-1)) \Longrightarrow \mathcal{A}(n)$$

holds. Note that for $n = 0$, this implication is saying that

$$\underbrace{(\text{nothing})}_{\substack{\text{tautology, i.e., a statement} \\ \text{that says nothing and thus is true}}} \qquad \Longrightarrow \mathcal{A}(0),$$

i.e., that $\mathcal{A}(0)$ holds unconditionally. So this is some kind of induction base folded into the induction step. In practice, when using strong induction, the induction step will often treat small values of n (like $n = 0$ and $n = 1$) differently from larger values, so we will get "de-facto base cases" inside the induction step.

Let us see how to prove Binet's formula using strong induction:

Proof of Binet's formula. We let $\mathcal{A}(n)$ be the statement

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

So we must prove that $\mathcal{A}(n)$ holds for all $n \geq 0$.

By strong induction, it suffices to show that

$$(\mathcal{A}(0) \wedge \mathcal{A}(1) \wedge \cdots \wedge \mathcal{A}(n-1)) \Longrightarrow \mathcal{A}(n)$$

To show this, we assume that $\mathcal{A}(0) \wedge \mathcal{A}(1) \wedge \cdots \wedge \mathcal{A}(n-1)$. In other words,

$$f_k = \frac{1}{\sqrt{5}}\varphi^k - \frac{1}{\sqrt{5}}\psi^k \qquad \text{for all } k < n.$$

We want to prove $\mathcal{A}(n)$, that is, we want to prove that

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

The definition of the Fibonacci numbers yields

$$\begin{aligned}
f_n &= f_{n-1} + f_{n-2} \\
&= \left(\frac{1}{\sqrt{5}}\varphi^{n-1} - \frac{1}{\sqrt{5}}\psi^{n-1}\right) + \left(\frac{1}{\sqrt{5}}\varphi^{n-2} - \frac{1}{\sqrt{5}}\psi^{n-2}\right) \\
&\qquad \left(\begin{array}{c}\text{by our induction hypothesis,} \\ \text{specifically by } \mathcal{A}(n-1) \text{ and } \mathcal{A}(n-2)\end{array}\right) \\
&= \frac{1}{\sqrt{5}}\varphi^{n-1} + \frac{1}{\sqrt{5}}\varphi^{n-2} - \frac{1}{\sqrt{5}}\psi^{n-1} - \frac{1}{\sqrt{5}}\psi^{n-2} \\
&= \frac{1}{\sqrt{5}}\varphi^{n-2} \underbrace{(\varphi+1)}_{\substack{=\varphi^2 \\ \text{(by computation)}}} - \frac{1}{\sqrt{5}}\psi^{n-2} \underbrace{(\psi+1)}_{\substack{=\psi^2 \\ \text{(by computation)}}} \\
&= \frac{1}{\sqrt{5}}\varphi^{n-2}\varphi^2 - \frac{1}{\sqrt{5}}\psi^{n-2}\psi^2 \\
&= \frac{1}{\sqrt{5}}\varphi^n - \frac{1}{\sqrt{5}}\psi^n.
\end{aligned}$$

That is, $\mathcal{A}(n)$ holds. This completes the induction step.

Right?

Careful: We have assumed $\mathcal{A}(0) \wedge \mathcal{A}(1) \wedge \cdots \wedge \mathcal{A}(n-1)$, and then we have applied $\mathcal{A}(n-2)$ and $\mathcal{A}(n-1)$. For this to work, we need to know that $n-2$ and $n-1$ belong to $\{0, 1, \ldots, n-1\}$. This, in turn, holds for all $n \geq 2$, but not for $n = 0$ or $n = 1$. So our above argument only works for $n \geq 2$. We thus need to do the cases $n = 0$ and $n = 1$ separately.

Fortunately, they are straightforward: for instance, the $n = 1$ case is checked by

$$\begin{aligned}
f_1 &= 1, \\
\frac{1}{\sqrt{5}}\varphi^1 - \frac{1}{\sqrt{5}}\psi^1 &= \frac{1}{\sqrt{5}}\varphi - \frac{1}{\sqrt{5}}\psi = \frac{1}{\sqrt{5}}\frac{1+\sqrt{5}}{2} - \frac{1}{\sqrt{5}}\frac{1-\sqrt{5}}{2} = 1.
\end{aligned}$$

The number φ is known as the **golden ratio** and we will meet it many times.

So much for algebraic properties of Fibonacci numbers. There are also combinatorial ones. Here is one:

Definition 1.0.2. A set S of integers is said to be **lacunar** if it contains no two consecutive integers (i.e., if there is no $s \in S$ such that $s + 1 \in S$).

For instance, $\{2, 4, 7\}$ is lacunar, but $\{2, 4, 5, 7\}$ is not.

Theorem 1.0.3. Let $n \geq 0$ be an integer. Let $[n]$ be the set $\{1, 2, \ldots, n\}$.

Then, the number of all lacunar subsets of $[n]$ is the Fibonacci number f_{n+2}.

Example 1.0.4. Let $n = 4$. The lacunar subsets of $[4]$ are

$$\varnothing, \quad \{1\}, \quad \{2\}, \quad \{3\}, \quad \{4\}, \quad \{1,3\}, \quad \{1,4\}, \quad \{2,4\}.$$

There are 8 of them, and of course $f_{4+2} = f_6 = 8$.

For comparison, the number of **all** subsets of $[n]$ is 2^n.

Proof of the theorem. Apply strong induction on n.

Assume that the theorem is true for $0, 1, \ldots, n-1$. We must prove that it is true for n.

This is easy to check by hand for $n = 0$ and for $n = 1$. So assume WLOG that $n \geq 2$.

A lacunar subset of $[n]$ either contains n or does not. So (the symbol "#" means "number")

$$\begin{aligned}
&(\text{\# of lacunar subsets of } [n]) \\
&= \underbrace{(\text{\# of lacunar subsets of } [n] \text{ that contain } n)}_{\substack{=(\text{\# of lacunar subsets of } [n-2]) \\ \text{(because the lacunar subsets of } [n] \text{ that contain } n \\ \text{are just the lacunar subsets of } [n-2] \text{ with the} \\ \text{extra element } n \text{ inserted into them)}}} \\
&\qquad + \underbrace{(\text{\# of lacunar subsets of } [n] \text{ that don't contain } n)}_{=(\text{\# of lacunar subsets of } [n-1])} \\
&= \underbrace{(\text{\# of lacunar subsets of } [n-2])}_{\substack{=f_{(n-2)+2} \\ \text{(by the induction hypothesis)}}} \\
&\qquad + \underbrace{(\text{\# of lacunar subsets of } [n-1])}_{\substack{=f_{(n-1)+2} \\ \text{(by the induction hypothesis)}}} \\
&= f_{(n-2)+2} + f_{(n-1)+2} = f_n + f_{n+1} = f_{n+2}.
\end{aligned}$$

This concludes the proof by strong induction. □

Induction can be useful even if there is seemingly nothing to induct on.

Exercise 7. Prove that

$$\sum_{i=1}^{\infty} \frac{1}{i\left(i+1\right)} = 1.$$

Solution. We have

$$\sum_{i=1}^{\infty} \frac{1}{i\left(i+1\right)} = \lim_{n\to\infty} S\left(n\right), \qquad \text{where } S\left(n\right) = \sum_{i=1}^{n} \frac{1}{i\left(i+1\right)}.$$

Maybe we can compute $S\left(n\right)$?

$$S\left(0\right) = 0, \qquad S\left(1\right) = \frac{1}{2}, \qquad S\left(2\right) = \frac{2}{3}, \qquad S\left(3\right) = \frac{3}{4}.$$

Thus, we suspect that

$$S\left(n\right) = \frac{n}{n+1} \qquad \text{for each } n \geq 0.$$

How do we prove such a suspicion? By induction on n, and in fact a very straightforward induction. (The induction step is

$$\begin{aligned} S\left(n\right) &= S\left(n-1\right) + \frac{1}{n\left(n+1\right)} = \frac{n-1}{\left(n-1\right)+1} + \frac{1}{n\left(n+1\right)} \\ &= \frac{n}{n+1} \qquad \text{(after a bit of computation)}. \end{aligned}$$

)

So

$$\sum_{i=1}^{\infty} \frac{1}{i\left(i+1\right)} = \lim_{n\to\infty} S\left(n\right) = \lim_{n\to\infty} \frac{n}{n+1} = \lim_{n\to\infty} \frac{1}{1+\frac{1}{n}} = \frac{\lim\limits_{n\to\infty} 1}{\lim\limits_{n\to\infty} 1 + \lim\limits_{n\to\infty} \frac{1}{n}} = \frac{1}{1+0} = 1.$$

Alternatively,

$$\sum_{i=1}^{\infty} \frac{1}{i\left(i+1\right)} = \lim_{n\to\infty} S\left(n\right) = \lim_{n\to\infty} \frac{n}{n+1} = \lim_{n\to\infty} \left(1 - \frac{1}{n+1}\right) = 1.$$

Exercise 8. Prove that the golden ratio $\varphi = \dfrac{1+\sqrt{5}}{2}$ satisfies

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}} = \varphi.$$

Note: The infinite nested fraction on the LHS is called an **(infinite) continued fraction**. Rigorously, it is defined as the limit

$$\lim_{n\to\infty}\left(\underbrace{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{\ddots+\cfrac{1}{1}}}}}}_{\text{with } n \text{ fractions}}\right).$$

Solution. Set

$$x_n := \underbrace{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{\ddots+\cfrac{1}{1}}}}}}_{\text{with } n \text{ fractions}} \qquad \text{for each } n \geq 0.$$

Thus,

$$x_0 = 1, \qquad x_1 = 1+\frac{1}{1} = 2, \qquad x_2 = 1+\cfrac{1}{1+\cfrac{1}{1}} = \frac{3}{2},$$

$$x_3 = 1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1}}} = 1+\frac{1}{x_2} = 1+\frac{1}{\left(\frac{3}{2}\right)} = 1+\frac{2}{3} = \frac{5}{3},$$

$$x_4 = 1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1}}}} = 1+\frac{1}{x_3} = 1+\frac{3}{5} = \frac{8}{5},$$

$$x_5 = 1+\frac{5}{8} = \frac{13}{8}.$$

So it looks like

$$x_n = \frac{f_{n+2}}{f_{n+1}} \qquad \text{for each } n \geq 0.$$

How do we prove this? We induct on n, using the recursion

$$x_n = 1 + \frac{1}{x_{n-1}} \qquad \text{for all } n \geq 1.$$

So to go from $n-1$ to n, we must just argue that

$$x_n = 1 + \frac{1}{x_{n-1}} = 1 + \frac{1}{\left(\frac{f_{n+1}}{f_n}\right)} = 1 + \frac{f_n}{f_{n+1}} = \frac{f_{n+1} + f_n}{f_{n+1}} = \frac{f_{n+2}}{f_{n+1}}.$$

OK, so we have now proved that

$$x_n = \frac{f_{n+2}}{f_{n+1}} \qquad \text{for each } n \geq 0.$$

Thus,

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} \frac{f_{n+2}}{f_{n+1}} = \lim_{n\to\infty} \frac{\frac{1}{\sqrt{5}}\varphi^{n+2} - \frac{1}{\sqrt{5}}\psi^{n+2}}{\frac{1}{\sqrt{5}}\varphi^{n+1} - \frac{1}{\sqrt{5}}\psi^{n+1}}$$

by Binet's formula. What now?

$$\begin{aligned}
\lim_{n\to\infty} x_n &= \lim_{n\to\infty} \frac{\frac{1}{\sqrt{5}}\varphi^{n+2} - \frac{1}{\sqrt{5}}\psi^{n+2}}{\frac{1}{\sqrt{5}}\varphi^{n+1} - \frac{1}{\sqrt{5}}\psi^{n+1}} = \lim_{n\to\infty} \frac{\varphi^{n+2} - \psi^{n+2}}{\varphi^{n+1} - \psi^{n+1}} \\
&= \lim_{n\to\infty} \frac{\varphi^{n+2}\left(1 - \rho^{n+2}\right)}{\varphi^{n+1}\left(1 - \rho^{n+1}\right)}, \qquad \text{where } \rho = \frac{\psi}{\varphi} \\
&= \varphi \cdot \lim_{n\to\infty} \frac{1 - \rho^{n+2}}{1 - \rho^{n+1}}.
\end{aligned}$$

But $\varphi \approx 1.618$ and $\psi \approx -0.618$, so $\rho = \frac{\psi}{\varphi} \approx \frac{-0.618}{1.618} = -0.382$; in any way, $|\rho| < 1$ (this follows from $\varphi > 1$ and $\psi \in (-1, 0)$). Thus, the powers of ρ converge to 0 as $n \to \infty$. Hence,

$$\lim_{n\to\infty} \frac{1 - \rho^{n+2}}{1 - \rho^{n+1}} = \frac{\lim_{n\to\infty} 1 - \lim_{n\to\infty} \rho^{n+2}}{\lim_{n\to\infty} 1 - \lim_{n\to\infty} \rho^{n+1}} = \frac{1-0}{1-0} = 1.$$

So

$$\lim_{n\to\infty} x_n = \varphi \cdot \underbrace{\lim_{n\to\infty} \frac{1 - \rho^{n+2}}{1 - \rho^{n+1}}}_{=1} = \varphi,$$

as desired.

Exercise 9. We say that a number is **funny** if it can be written in the form

$$\pm 1^2 \pm 2^2 \pm 3^2 \pm \cdots \pm m^2$$

for some nonnegative integer m and some choice of $\pm$ signs. For example, 4 is funny because $4 = -1^2 - 2^2 + 3^2$. Also, 0 is funny because we can take $m = 0$ and get the empty sum.

Prove that every integer is funny.

Solution. If we cannot solve a problem directly, we can try to simplify it and solve the simpler problem first.

Here, we can try to replace the squares by first powers. So let's say that a number is **giggly** if it can be written in the form

$$\pm 1 \pm 2 \pm 3 \pm \cdots \pm m$$

for some nonnegative integer m and some choice of $\pm$ signs. Is every integer giggly?

For instance, 3 is giggly since $3 = 1 + 2$.

Is 4 giggly? Yes, since $4 = -1 + 2 + 3$.

Is 5 giggly? Yes, since $5 = 1 + 2 + 3 + 4 - 5$.

Is 6 giggly? Yes, since $6 = 1 + 2 + 3$.

If n is giggly, then so is $n + 1$, since $n = \pm 1 \pm 2 \pm 3 \pm \cdots \pm m$ entails

$$n + 1 = \pm 1 \pm 2 \pm 3 \pm \cdots \pm m - (m + 1) + (m + 2).$$

So, by induction, all $n \geq 0$ are giggly (since 0 is giggly).

What about negative integers? These are giggly, too, since you can flip all signs in $n = \pm 1 \pm 2 \pm 3 \pm \cdots \pm m$ to get $-n = \mp 1 \mp 2 \mp 3 \mp \cdots \mp m$.

So we have solved the simplified problem: We have shown that all integers are giggly.

Now what about the original problem? Why is every integer funny (i.e., of the form $\pm 1^2 \pm 2^2 \pm 3^2 \pm \cdots \pm m^2$)?

We try something similar as for the simplified problem: an argument for why n funny entails $n + 1$ funny.

Sadly, $-(m + 1)^2 + (m + 2)^2 = 2m + 3 \neq 1$.

Maybe we can find a pattern involving several (say, three or four) consecutive squares such that if we add them with signs, we get a constant? Yes:

$$(m + 1)^2 - (m + 2)^2 - (m + 3)^2 + (m + 4)^2 = 4.$$

Thus, if n is funny, then $n + 4$ is funny.

Hence, if we can show that $-1, 0, 1, 2$ are funny, then so is every nonnegative integer (by strong induction), and therefore every integer (since we can go from n to $-n$ by flipping all the signs).

But this is easy:

$$0 = (\text{empty sum}), \qquad 1 = +1^2, \qquad 2 = -1^2 - 2^2 - 3^2 + 4^2,$$
$$-1 = -1^2.$$

So the problem is solved.