Math 2001. Lecture 31.

04. 11. 2022.

Last time:

- more strong induction proofs; graphs and trees.

Today:

- Another strong induction proof:

  fundamental thm of arithmetic / prime decomp. of integers

- Induction proofs about Fibonacci numbers.

1. The fundamental thm of arithmetic

Thm: Every positive integer $n>1$ has a unique factorization into prime numbers (up to reordering of the factors).

E.g. $60 = 2\times 3\times 2\times 5 = 2\times 2\times 3\times 5$.

Pf: We first prove existence of such a prime decomposition by strong induction on n.

Base case: $n=2$. Since 2 is a prime $2=2$ is the prime decomp of 2.

Inductive step: Suppose we have proven that $2, 3, 4, \cdots, k$ all have prime decomp for some k. We want to prove that $n := k+1$ also has a prime decomp.

- If n is itself a prime, then $n=n$ is a prime decomp of n.
- If n is not prime, then n has two divisors a, b s.t. $1<a, b<n$ and $n=ab$.

In this case, by the strong inductive hypothesis, both a and b have prime decomp, say $a = p_1 p_2 \cdots p_r$, $b = p_1' p_2' \cdots p_s'$ where each p_i and p_j' is prime. Then $n = ab = p_1 p_2 \cdots p_r p_1' p_2' \cdots p_s'$, which gives a prime decomp of n, as desired.

Next we prove the uniqueness of the prime factorization, again via strong induction:

Base case: $n = 2$. It's clear that $2 = 2$ is the only prime decomp. of n.

Inductive step (combined with "proof by contradiction"): Suppose, for contradiction, that some number in $\mathbb{Z}_{\geq 1}$ does not have a unique prime decomp. Then there's a minimal such number, n, having at least two prime decomp. We will derive a contradiction.

"pf by smallest counterexample"

To do so, suppose n has different prime decomps

$$n = a_1 \cdot a_2 \cdot \cdots \cdot a_\ell = p_1 \cdot \cdots \cdot p_k .$$

($n = a_1 a_2 \cdots a_\ell = p_1 p_2 \cdots p_k$) Since $p_1 \mid n = a_1 a_2 \cdots a_\ell$, it follows that

$p_1 \mid a_i$ for some $1 \le i \le \ell$, which in turn implies that $p_1 = a_i$ since a_i is prime.

But then we have

$$n = p_1 (p_2 \cdots p_k) = a_1 a_2 \cdots a_\ell = a_i (a_1 a_2 \cdots a_{i-1} a_{i+1} \cdots a_\ell).$$

It follows that $p_2 \cdots p_k = a_1 a_2 \cdots a_{i-1} a_{i+1} \cdots a_\ell$ are two different prime decomps of the integer $n' := n/p_1 = n/a_i$. But then n' is a smaller integer in $\mathbb{Z}_{\geq 2}$ that have more than one prime decomps, contradicting the minimality assumption that n is the smallest int in $\mathbb{Z}_{\geq 2}$ with more than one prime decomp. $\square$

2. Fibonacci numbers

Def: The Fibonacci sequence is the recursively define sequence $F_1, F_2, F_3, \cdots$ given by the initial values $F_1 = 1$, $F_2 = 1$ and the recursion

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

(**e.g.** $F_3 = F_1 + F_2 = 1+1 = 2$. $F_4 = F_2 + F_3 = 1+2 = 3$.

$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \cdots\cdots$)

The numbers in the sequence are called Fibonacci numbers.

Rmk: The recursive nature of the Fibonacci sequence allows inductive proof for many properties of Fibonacci numbers.

Prop: The Fibonacci sequence satisfies $\underbrace{F_{n+1}^2 - F_{n+1}F_n - F_n^2}_{S_n} = (-1)^n$ (*) $\forall n \geq 1$.

E.g. 1, 1, 2, 3, 5, 8, 13, ...

$n=1$ $\quad F_2^2 - F_2F_1 - F_1^2 = 1^2 - 1\cdot 1 - 1^2 = -1 = (-1)^1$.

$n=2$ $\quad F_3^2 - F_3F_2 - F_2^2 = 2^2 - 2\cdot 1 - 1^2 = 4-2-1 = 1 = (-1)^2$

$n=3$ $\quad F_4^2 - F_4F_3 - F_3^2 = 3^2 - 3\cdot 2 - 2^2 = 9-6-4 = -1 = (-1)^3$.

Pf: We use induction on n.

Base case: $n=1$.

$n=2$. $\quad$ ... (*) holds by the direct computations.

for the Fibonacci sequence, we should ~~almost~~ almost always check <u>two</u> base cases $n=1, n=2$ because the recursion $F_n = F_{n-1} + F_{n-2}$ only "kicks in" for $n \geq 3$.

Inductive step: Suppose (*) holds for all $n=1, n=2, \ldots, n=k$ for some $k\geq 1$.

We want to show that (*) must also hold for $n=k+1$:

$$\left.\left(F_{n+1}^2 - F_{n+1}F_n - F_n^2\right)\right|_{n=k+1} = F_{(k+1)+1}^2 - F_{(k+1)+1}F_{k+1} - F_{k+1}^2$$

$$= F_{k+2}^2 - F_{k+2}F_{k+1} - F_{k+1}^2$$

$$\stackrel{\text{Fib. recursion}}{=} \left(F_{k+1}+F_k\right)^2 - \left(F_{k+1}+F_k\right)F_{k+1} - F_{k+1}^2$$

$$= \underline{F_{k+1}^2} + \underline{2F_{k+1}F_k} + F_k^2 - \underline{F_{k+1}^2} - \underline{F_kF_{k+1}} - \underline{F_{k+1}^2}$$

$$= -F_{k+1}^2 + F_{k+1}F_k + F_k^2$$

$$= -\left(F_{k+1}^2 - F_{k+1}F_k - F_k^2\right) \underset{S_k}{\overset{\text{ind. hyp.}}{=\!=}} -(-1)^k = (-1)^{k+1}$$

It follows that S_n holds, i.e., (*) holds, for all $n\geq 1$.

$\square$