5.4 Strong Induction

Cliff Sun

February 26, 2024

Midterm 2 next week $\rightarrow$ chapters 4 to 6

Fibnacci numbers:

$$f_{n+1} = fn + f_{n-1} \tag{1}$$

When is f_n even? Conjecture: every 3rd number in the sequence is even.

$$f_n \text{ is even} \iff 3|n \tag{2}$$

Regular induction:

$$p(n) \implies p(n+1) \tag{3}$$

But this doesn't really work since the fib numbers rely on the previous 2 numbers.
Motivation $\rightarrow$ try to create a new form of induction that satisfies the following:

$$(p(n) \land p(n-1) \implies p(n+1)) \tag{4}$$

This means that we must prove that $p(1)$ and $p(2)$ are true. For intuition, think of this as a ladder, meaning that if $p(3)$ is true, and $p(2)$ is also true, then $p(4)$ is true, and etc.

(Principle of Strong Induction). Let $n \in \mathbb{Z}$ and suppose that $P(n)$ is a propositional function for
$n \in \mathbb{Z}$ for some n greater than or equal to m. Suppose that for some $l \geq m$:
1. $p(n)$, $p(n+1)$, etc.. $p(l)$ are true
2. $\forall n \in l \ p(m) \land p(m+1) \cdots \land p(n) \implies p(n+1)$
3. Then $p(n)$ is true for all $n \in \mathbb{Z}$

The differences between regular induction is that you start at $n = m$ and that you assume all the cases up to $p(n)$, not just $p(n)$

Strong Induction allows for the possibility that regular induction doesn't work straight from the beginning, so you choose to "offload" the base cases to include the sections that don't work.
In this case, l is the last case that the induction doesn't work. This allows for induction on cases where instability is seen in the very beginning of the relationship, but stabilizes for larger n's.

Conjecture: $\forall n \in \mathbb{N}$, f_n is even $\iff$ 3—n.

Proof. We will use strong induction for this proof. Let the propositional function $p(n)$ be the statement that "f_n is even $\iff$ 3—n". Let's begin by checking the base cases $p(1)$ and $p(2)$.
$p(1)$: f_1 is even if 3—1.
$p(2)$: f_2 is even if 3—2.
Thus, we have proved the base cases.
For the inductive step, suppose that

$$p(n-1) \land p(n) \text{are true.} \tag{5}$$

We claim that $p(n+1)$ is true.

Consider 3 cases:
1. $n \equiv 0 \pmod 3$. Then our inductive hypothesis states that f_n is even and f_{n-1} is odd. Then f_{n+1} is odd.

So the statement that $p(n+1)$ is that "f_{n+1} is even $\iff$ 3—(n+1)"
2. $n \equiv 1 \pmod 3$. This states that f_n is odd and f_{n-1} is even. Thus f_{n+1} is odd which implies that 3 does not divide $n+1$. But that works since we know that n is divisible by 3, so that works out.
3. $n \equiv 2 \pmod 3$. This states that f_n is odd and that f_{n-1} is also odd. Thus 3 divides $n+1$, so $n+1$ must be even.

Thus, $p(n+1)$ is true for all cases, thus by induction, the theorem is true. $\square$

Proof about division algorithm. Conjecture: the division algorithm states that if $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, then there exists unique numbers $q, r \in \mathbb{Z}$ such that
1. $0 \le r < n$
2. $m = nq + r$
We'll prove that if m is non-negative and $n = 5$, then there exists integers q, r satisfying (1.) and (2.). Shorthand is that 'm can be divided by 5 with a remainder of r'.

Proof. We will use strong induction for this proof just on m. Our base cases for m are the numbers from 0 to 4. That is

$$0 \le m < 5 \tag{6}$$

Then m can be divided by 5 with a remainder

$$m = 5 \cdot 0 + r \tag{7}$$

For the inductive step, suppose that we're given some value of $m \ge 5$ such that every $m' \in \{0, \ldots, m-1\}$ can be divided by 5 with remainder.
By assumption, we can write that

$$m - 5 = 5q' + r' \tag{8}$$

For some integers q' and r' with $0 \le r < 5$. Then

$$m = 5(q' + 1) + r' \tag{9}$$

So m can be divded by 5 with remainder. By strong induction, this proves the theorem. $\square$

Theorem: every integer n $\ge$ 2 can be expressed as the product of one or more primes.

Proof. We will proceed by strong induction. With no base cases, suppose that n is an integer greater than 1 such that every integer n' in the range 2 up to $n-1$ can be expressed as a product of primes. Then we must prove that n can be too. Consider 2 cases:

1. n is prime, then n is a product of 1 prime.
2. n is not prime, then $n = a \cdot b$ where a and b are in the range of 2 up to m - 1. But a and b can be written as a product of primes. Thus n can also be written as a product of primes.

$\square$