What are “Numbers”?

Here we are following in the footsteps of Richard Dedekind (1831–1916). I'll encapsulate his ideas in a

Friendly Definition of $\mathbb{Z}$

$\mathbb{Z}$ is a set equipped with

- an equivalence relation "$=$"
  - $\forall a \in \mathbb{Z}$, $a = a$,
  - $\forall a, b \in \mathbb{Z}$, $a = b \Rightarrow b = a$,
  - $\forall a, b, c \in \mathbb{Z}$, $a = b$ and $b = c \Rightarrow a = c$.
- a total ordering "$\leq$"
  - $\forall a, b \in \mathbb{Z}$, $a \leq b$ and $b \leq a \Rightarrow a = b$,
  - $\forall a, b, c \in \mathbb{Z}$, $a \leq b$ and $b \leq c \Rightarrow a \leq c$,
  - $\forall a, b \in \mathbb{Z}$, $a \leq b$ or $b \leq a$.
- two binary operations
  $+ : \mathbb{Z}^2 \to \mathbb{Z}$
  $\times : \mathbb{Z}^2 \to \mathbb{Z}$
- two special elements $0, \underline{1} \in \mathbb{Z}$

satisfying appoximately twelve axioms.

(See the handout.)

Eleven of the axioms are fairly obvious, but there is one axiom that is fairly subtle. It took a long time for people to realize that this is an axiom and not a theorem.

☆ Axiom of Well-Ordering:

Every non-empty set of positive (or non-negative; it's not important) integers has a smallest element.

Formally: $\forall X \subseteq \mathbb{N}$ such that $X \neq \emptyset$, $\exists x \in X$ such that $\forall y \in X$, $x \leq y$.

[Remark: While the first 11 axioms are "algebraic", the well-ordering property is "logical" in nature.]

Yes, indeed, we needed well-ordering in our proof of the Division Theorem (look back and see).

Now our definition of $\mathbb{Z}$ is complete. ///.

Dedekind did this in 1888.
Giuseppe Peano (1858–1932) came along in 1889 and compactified Dedekind's definition.

Peano's Definition of $\mathbb{N}$

$\mathbb{N}$ is a set equipped with

- an equivalence relation "="
- a function $S : \mathbb{N} \to \mathbb{N}$
- a special element $0 \in \mathbb{N}$

satisfying just <u>three</u> <u>axioms</u>:

1. $\forall n \in \mathbb{N}$, $S(n) \neq 0$.
2. $\forall m, n \in \mathbb{N}$ we have

$$S(m) = S(n) \implies m = n.$$

3. If a set $X \subseteq \mathbb{N}$ satisfies
   - $0 \in X$
   - $\forall n \in \mathbb{N}$, $n \in X \Rightarrow S(n) \in X$.

   then it follows that $X = \mathbb{N}$.

//

Remarks on Peano:

- We are supposed to think

$$S(n) = \text{"}n+1\text{"}$$

(S is for "successor").

- The third axiom is called the principle (or axiom) of induction. It is logically equivalent to well-ordering but we probably won't prove this.

- Induction is subtle in the friendly definition (we almost missed it!) but it becomes the very heart of Peano's definition

Moral of the story:

It is not obvious, but

$$\text{principle of induction} \equiv \text{concept of number}$$

//

Back to earth. How is induction used?

Example: Prove that for all integers $n \geq 1$ we have

$$2^{n-1} \leq n!$$

First let's test it.

$n = 1$ $\quad 2^0 = 1 \leq 1! = 1$ ✓

$n = 2$ $\quad 2^1 = 2 \leq 2! = 2$ ✓

$n = 3$ $\quad 2^2 = 4 \leq 3! = 6$ ✓

$n = 4$ $\quad 2^3 = 8 \leq 4! = 24$ ✓

Ok, I believe it. Now what?

Idea: I'll ask my computer to check it. My computer proves that it's true for all $n \leq 10^{1000000000000}$. Then my computer breaks down.

OK, now what? We're supposed to prove it for <u>all</u> integers $n \geq 1$, not just "a lot" of them.

Do you see that this is impossible without some extra help?

Let's think abstractly. Suppose, hypothetically, that we have some integer $k \geq 1$ such that

$$2^{k-1} \leq k! \qquad (*)$$

What logical consequences does this have (again, hypothetically)?

I can do lots of things.... like

$$2^{k-1} \leq k!$$
$$2 \cdot 2^{k-1} \leq 2 \cdot k!$$
$$2^{k} \leq 2 \cdot k!$$

But wait a minute! Isn't

$$2 \cdot k! \leq (k+1) \cdot k! \quad ?$$
$$2 \cdot k! \leq (k+1)! \quad ?$$

Certainly if (hypothetically) we have $2 \leq k+1$, then it follows that

$$2 \leq k+1$$
$$2 \cdot k! \leq (k+1) \cdot k!$$
$$2 \cdot k! \leq (k+1)!$$

OK great. Put it together:

If $k \geq 1$ and $2^{k-1} \leq k!$, then we have

$$2^{k-1} \leq k!$$
$$2 \cdot 2^{k-1} \leq 2 \cdot k!$$
$$2^{k} \leq 2 \cdot k! \leq (k+1)!$$

Hence $2^{k} \leq (k+1)!$

You can imagine repeating the same argument to show that

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

Q: It looks good. Are we done?

A: I don't know. Are we?

I think we both agree that this is a proof, but we should draw up a legal contract, just in case.

☆ The Axiom of Induction:

Consider a statement $P : \mathbb{N} \to \{T, F\}$ about natural numbers. If

- $P(b) = T$ for some $b \in \mathbb{N}$

and

- For any $k \geq b$ we have that
$$P(k) \Rightarrow P(k+1)$$

then we will <u>agree</u> to say that

$$P(n) = T \text{ for } \underline{\text{all}}\ n \geq b.$$

(Please sign here.)

Now let's write up our proof in the legal way.

Theorem: Given $n \in \mathbb{N}$ we define the statement

$$P(n) := \text{“ } 2^{n-1} \leq n! \text{ ”}$$

We claim that $P(n) = T$ for all $n \geq 1$.

Proof: We will use induction.

First we verify the base case. Note that $2^{1-1} = 2^0 = 1$ and $1! = 1$, hence

$$P(1) = \text{“ } 2^{1-1} \leq 1! \text{ ”} = T.$$

Next we verify the "induction step". Suppose (hypothetically) that we have some $k \geq 1$ such that $P(k) = T$, i.e., such that

$$2^{k-1} \leq k!$$

In this case, since $k+1 \geq 2$, it follows that

$$2^{k-1} \leq k!$$
$$2 \cdot 2^{k-1} \leq 2 \cdot k!$$
$$2^k \leq 2 \cdot k! \leq (k+1)\, k!$$
$$2^k \leq (k+1)\, k!$$
$$2^k \leq (k+1)!$$

and hence $P(k+1) = T$. We have proved that for all $k \geq 1$ we have

$$P(k) \Longrightarrow P(k+1)$$

(hypothetically, of course :))

By the Axiom of Induction, we conclude that $P(n) = T$ for <u>all</u> $n \geq 1$.

//

You may think you understand what we did here, but a word of warning:

Be careful to use the Axiom of Induction exactly as written, or <u>I</u> might sue you!

Getting Serious with Induction

Recall the

Principle of Induction:

Consider a function $P : \mathbb{N} \to \{T, F\}$.
If

(1) $P(b) = T$ for some $b \in \mathbb{N}$

and

(2) $P(k) \Rightarrow P(k+1)$ for all $k \geq b$

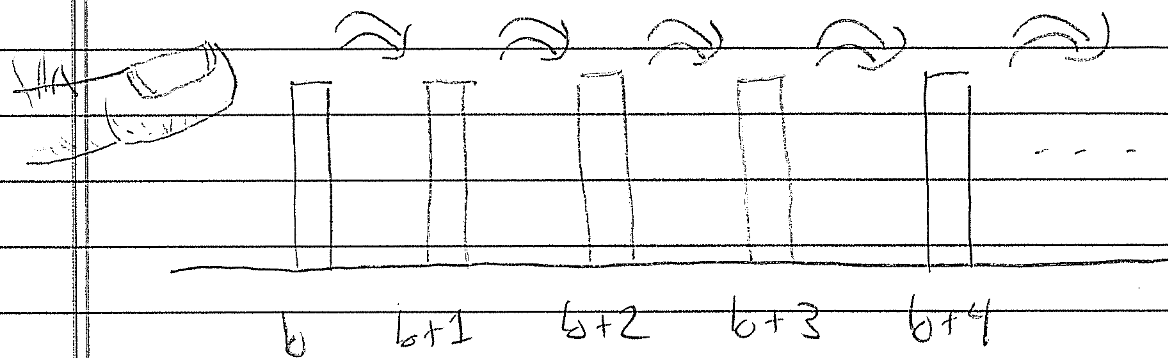
then we agree to say that

$$P(n) = T \text{ for } \underline{\text{all}}\ n \geq b.$$

Last time I gave an analogy of a computer trying to verify that $P(n) = T$ for all $n \geq b$ and breaking down because of the 2nd law of thermodynamics or some such thing.

Here's a different analogy:

induction $\equiv$ dominoes



(1) Your finger.

(2) The force of gravity

Both are necessary to this process.

Here's a cautionary example:

We say that a set of horses is monochromatic if all the horses in the set have the same color.

Theorem:

Every (finite) set of horses is monochromatic. (In other words, all horses have the same color.)

Proof by Induction:

Given $n \in \mathbb{N}$ let

$P(n) =$ "Every set of n horses is monochromatic"

First we verify the base case. Clearly every set of 1 horse is monochromatic, so

$$P(1) = T.$$

Next we verify the induction step. Assume (hypothetically) that $P(k) = T$, i.e., every group of k horses is monochromatic. In this case we want to show that $P(k+1) = T$.

So consider any set S of $k+1$ horses and consider any two horses $x, y \in S$. We will show that x and y have the same color.

To do this, let $z \in S$ be any third horse.

Since the set $S - \{y\}$ has size k we know by assumption that $S-\{y\}$ is monochrom. Then since $x, z \in S - \{y\}$ we know that x & z have the same color.

Similary, we know that $S - \{x\}$ is monochrom. Then since $y, z \in S - \{x\}$ we know that y & z have the same color.

By transitivity we conclude that x & y have the same color. Since this is true for any $x, y \in S$ we conclude that S is monochromatic. Since this is true for any set S of $k+1$ horses we conclude that

$P(k+1) = T$ as desired.

We have thus proved that

$$P(k) \Longrightarrow P(k+1).$$

By the principle of induction we conclude that $P(n) = T$ for <u>all</u> $n \geq 1$.

In other words, all horses have the same color.

OK, so clearly we made a mistake, but what <u>EXACTLY</u> was the mistake ??

We <u>successfully</u> showed that

(1) $P(1) = T$

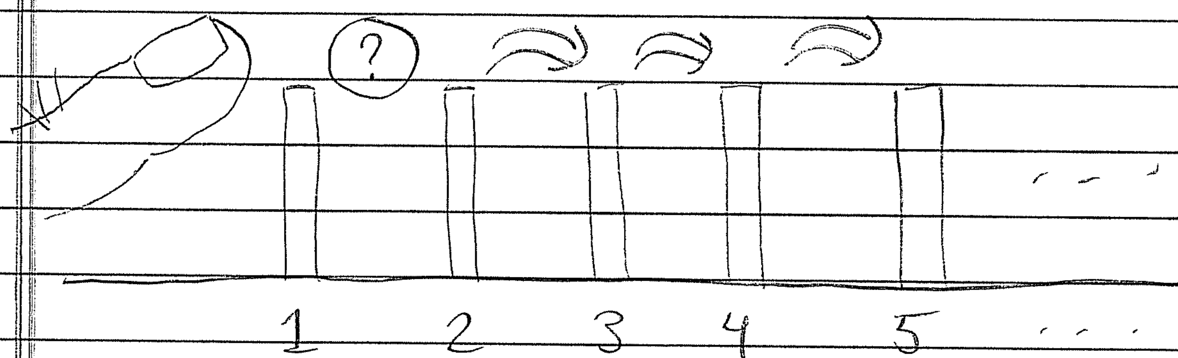
and

(2) For all $k \geq 2$ we have

$$P(k) \Longrightarrow P(k+1).$$

(Yes, our argument that $P(k) \Rightarrow P(k+1)$ implicitly used the assumption that $k \geq 2$ when we said "let $z \in S$ be any third horse". What if there is no third horse? Then our argument falls apart.)

Here's the situation:



The finger is OK but there is a small problem with gravity; namely, there is NO GRAVITY between dominoes 1 and 2. So only domino 1 will fall down. The rest remain standing.

If we could somehow prove $P(2) = T$ then the rest would fall down.

So close, and yet so far...

Practice With Induction

Using induction takes practice, so this week we will practice.

__Definition:__ Given integers $n, d \in \mathbb{Z}$ we define the statement

$$\text{“}d \mid n\text{”} := \text{“}\exists k \in \mathbb{Z};\ n = dk\text{”}$$

We read "$d \mid n$" as "d divides n" or "n is divisible by d".

__Problem:__ Prove that for all $n \in \mathbb{N}$ we have

$$6 \mid (2n^3 + 3n^2 + n).$$

__Proof:__ For all $n \in \mathbb{N}$ define the statement

$$P(n) := \text{“}6 \mid (2n^3 + 3n^2 + n)\text{”}.$$

Base Case:

$$P(0) = \text{“}6 \mid (2 \cdot 0^3 + 3 \cdot 0^2 + 0)\text{”} = \text{“}6 \mid 0\text{”}$$

Is this true?

Yes. Recall that

"$6 \mid 0$" = "$\exists k \in \mathbb{Z},\ 0 = 6k$".

This is true because we can take $k = 0$.

[You should check a few more cases, $P(1), P(2), P(3)$ just to make sure you believe the result, but it's not strictly necessary for the proof.]

Induction Step: Consider any $k \geq 0$ and "assume for induction" that $P(k) = T$, i.e., assume that there exists $d \in \mathbb{Z}$ such that

$$2k^3 + 3k^2 + k = 6d.$$

In this case we want to show that $P(k+1) = T$, i.e., that

$$6 \mid \left[2(k+1)^3 + 3(k+1)^2 + (k+1)\right]$$

OK, now what?

Probably we should expand.

$$2(k+1)^3 + 3(k+1)^2 + (k+1)$$

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

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

$$= 2k^3 + 9k^2 + 13k + 6$$

OK, now what?

Somehow we must use the fact that

$$2k^3 + 3k^2 + k = 6d \ldots\ldots$$

I guess we went too far. Back up.

$$2(k+1)^3 + 3(k+1)^2 + (k+1)$$

$$= \underbrace{(2k^3+3k^2+k)} + 6k^2 + 12k + 6$$

$$= 6d + 6k^2 + 12k + 6$$

$$= 6(d+k^2+2k+1) = 6\,(\text{something}).$$

We conclude that

$$P(k+1) = \text{“} 6 \mid \left[2(k+1)^3 + 3(k+1)^2 + (k+1)\right] \text{”} = T$$

as desired. In summary we have shown that for all $k \geq 0$ we have

$$P(k) \Rightarrow P(k+1).$$

End of induction step.

By the principle of Induction we conclude that

$$P(n) = T \text{ for all } n \geq 0.$$

//

[Thinking Problem: In fact, it is true that

$$6 \mid (2n^3 + 3n^2 + n)$$

for all $n \in \mathbb{Z}$ (including negative n). How would you prove this?]

Another Problem: Let

$F_n :=$ The set of binary strings of length n in which no two 1's are consecutive.

Find a formula for $\# F_n$.

Experiment:

$F_0 = \{\emptyset\}$

$F_1 = \{0, 1\}$

$F_2 = \{00, 01, 10\}$

$F_3 = \{000, 100, 010, 001, 101\}$

$F_4 = ?$

0000 1010
1000 1001
0100 0101
0010 That's All.
0001

Define $f_n := \# F_n$. We have

n	0	1	2	3	4	5
f_n	1	2	3	5	8	...

Can you guess a formula yet?
If not, we need more data.

n	4	5	6	7	8	9	10	...
f_n	8	13	21	34	55	89	144	...

Can you guess a formula yet? No.

OK, but maybe we can see a pattern or some structure?

Eventually we will observe the following fact: For all $n \geq 2$ we have

$$\boxed{f_n = f_{n-1} + f_{n-2}}$$

Why is this true?

<u>Proof</u>: We can write F_n as a disjoint union of two sets

$$F_n = A \sqcup B \quad , \text{ where}$$

$$A = \{ x \in F_n : x \text{ begins with } 0 \}$$

$$B = \{ x \in F_n : x \text{ begins with } 1 \}.$$

I claim that

$$\# A = f_{n-1}.$$

Indeed, if the first symbol is 0, then the rest of the word is an element of F_{n-1}

$$\underline{0}\ \underbrace{\boxed{\text{an element of } F_{n-1}}}_{\text{length } n-1} \in A.$$

We get a 1-1 correspondence $A \leftrightarrow F_{n-1}$ and hence $\# A = \# F_{n-1} = f_{n-1}$.

I also claim that

$$\# B = f_{n-2} .$$

Indeed, if the first symbol is 1 then the second symbol <u>must</u> be 0 (since there are no consecutive 1's. Then the rest of the word is an element of F_{n-2}

$$\underline{1}\ \underline{0}\ \underbrace{\boxed{\text{an element of } F_{n-2}}}_{\text{length } n-2} \in B$$

We get a 1-1 correspondence $B \leftrightarrow F_{n-2}$ and hence $\# B = \# F_{n-2} = f_{n-2}$.

We conclude that

$$\begin{aligned} f_n = \# F_n &= \# A + \# B \\ &= f_{n-1} + f_{n-2} \end{aligned}$$

Example:

$$F_4 = \left\{ \begin{array}{c} 0000 \\ 0100 \\ 0010 \\ 0001 \\ 0101 \end{array} \quad \begin{array}{c} 1000 \\ 1010 \\ 1001 \end{array} \right\}$$

$$f_4 = f_3 + f_2$$

$$8 = 5 + 3$$

OK great. Does that help us find a formula?

Maybe not, but if we can <u>guess</u> a formula, this will help us <u>prove</u> it.

I will give you the guess for free!

Let $\alpha := \dfrac{1+\sqrt{5}}{2}$ and $\beta := \dfrac{1-\sqrt{5}}{2}$

Then (Guess): For all $n \geq 0$ we have

$$f_n = \frac{1}{\sqrt{5}}\left(\alpha^{n+2} - \beta^{n+2}\right)$$

$$= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+2}\right]$$

Can you prove this using induction?

Fibonacci and Strong Induction

Today: More induction.

Last time we considered a problem:

Let $F_n :=$ The set of binary strings of length n in which no two 1's are consecutive.

Let $f_n := \# F_n$.

Find a "formula" for f_n.

Last time we found some data

n	0	1	2	3	4	5	6	$\cdots$
f_n	1	2	3	5	8	13	21	$\cdots$

We guessed the "recurrence formula"

$$f_n = f_{n-1} + f_{n-2} ,$$

then we proved it.

But we would still like a "closed formula"

$$f_n = \ ?$$

Two separate issues:

1. Can we guess a formula?

2. Given a proposed formula, can we prove it?

Let's skip issue 1 for now. I'll just tell you the formula and then we'll prove it.

☆ I claim that for all $n \in \mathbb{N}$ we have

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+2}\right]$$

That's pretty <u>surprising</u>, so we should check it before we try to prove it.

$n = 0$.

$$f_0 \stackrel{?}{=} \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2\right]$$

$$= \frac{1}{\sqrt{5}}\left[\frac{(1+\sqrt{5})^2}{4} - \frac{(1-\sqrt{5})^2}{4}\right]$$

$$= \frac{1}{4\sqrt{5}}\left[(\cancel{1}+2\sqrt{5}+\cancel{5}) - (\cancel{1}-2\sqrt{5}+\cancel{5})\right]$$

$$= \frac{1}{\cancel{4\sqrt{5}}}(\cancel{4\sqrt{5}}) = 1. \quad \checkmark$$

$n = 1$.

$$f_1 \stackrel{?}{=} \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^3 - \left(\frac{1-\sqrt{5}}{2}\right)^3\right]$$

$$= \frac{1}{\sqrt{5}}\left[\frac{(1+\sqrt{5})^3}{8} - \frac{(1-\sqrt{5})^3}{8}\right]$$

$$\vdots$$

$$= \frac{1}{8\sqrt{5}} \left[(1+\sqrt{5})^3 - (1-\sqrt{5})^3 \right]$$

$$= \frac{1}{8\sqrt{5}} \left[\left(\cancel{1} + 3\sqrt{5} + \cancel{3\cdot 5} + 1\cdot 5\sqrt{5}\right) - \left(\cancel{1} - 3\sqrt{5} + \cancel{3\cdot 5} - 1\cdot 5\sqrt{5}\right) \right]$$

$$= \frac{1}{8\sqrt{5}} \left(3\sqrt{5} + 5\sqrt{5} + 3\sqrt{5} + 5\sqrt{5} \right)$$

$$= \frac{1}{8\sqrt{5}} \left(16\sqrt{5} \right) = 2 \quad \checkmark$$

Wow, I really don't want to check any more.

Can we just say we believe it now?

Good. Now let's try to prove it by induction. I recommend that we hide the details inside some convenient notation.

Consider the quadratic equation

$$x^2 - x - 1 = 0.$$

Its solutions are

$$x = \frac{1 \pm \sqrt{(-1)^2 - 4 \cdot 1 \cdot (-1)}}{2} = \frac{1 \pm \sqrt{5}}{2}.$$

Let $\alpha := \frac{1+\sqrt{5}}{2}$ and $\beta := \frac{1-\sqrt{5}}{2}$.

[Remark: α is called the "golden ratio".]

By definition we have

$$\alpha^2 - \alpha - 1 = 0 \quad \text{and} \quad \beta^2 - \beta - 1 = 0$$
$$\alpha^2 = \alpha + 1 \qquad\qquad \beta^2 = \beta + 1.$$

This will be useful for hiding details.

Now we claim that

$$f_n = \frac{1}{\sqrt{5}} \left[\alpha^{n+2} - \beta^{n+2} \right].$$

What's the induction step?

Assume that $f_k = \frac{1}{\sqrt{5}}\left[\alpha^{k+2} - \beta^{k+2}\right]$.

We want to show $f_{k+1} = \frac{1}{\sqrt{5}}\left[\alpha^{k+3} - \beta^{k+3}\right]$.

OK, let's see. We have

$$\frac{1}{\sqrt{5}}\left[\alpha^{k+3} - \beta^{k+3}\right]$$

$$= \frac{1}{\sqrt{5}}\left[\alpha^{k+1}\alpha^{2} - \beta^{k+1}\beta^{2}\right]$$

$$= \frac{1}{\sqrt{5}}\left[\alpha^{k+1}(\alpha+1) - \beta^{k+1}(\beta+1)\right]$$

$$= \frac{1}{\sqrt{5}}\left[\alpha^{k+2} + \alpha^{k+1} - (\beta^{k+2} + \beta^{k+1})\right]$$

$$= \frac{1}{\sqrt{5}}\left[\alpha^{k+2} - \beta^{k+2}\right] + \frac{1}{\sqrt{5}}\left[\alpha^{k+1} - \beta^{k+1}\right]$$

$$= f_k + f_{k-1} \quad ??$$

Do we know this?

Well, we assumed that

$$f_k = \frac{1}{\sqrt{5}}\left[\alpha^{k+2} - \beta^{k+2}\right].$$

Why don't we also assume that

$$f_{k-1} = \frac{1}{\sqrt{5}}\left[\alpha^{k+1} - \beta^{k+1}\right] ?$$

Then, assuming these two facts, we get

$$\frac{1}{\sqrt{5}}\left[\alpha^{k+3} - \beta^{k+3}\right]$$

$$= f_k + f_{k-1} \quad \text{by assumption}$$

$$= f_{k+1} \quad \text{by the recurrence we proved.}$$

I guess that does it,

but we're going to need a new legal contract for the extra assumption we made.

★ Principle of Strong Induction :

Consider a function $P : \mathbb{N} \to \{T, F\}$. If

1. $P(b) = P(b+1) = \cdots = P(b+d-1) = T$

and 2. For all $k \geq b$ we have

$$(P(k) \wedge P(k+1) \wedge \cdots \wedge P(k+d-1)) \implies P(k+d)$$

then we agree to say that

$$P(n) = T \quad \forall\ n \geq b .$$

(Please sign here.) //

In essence, we are allowed to assume the d previous cases, as long as we check d base cases.

The usual Principle of Induction corresponds to $d = 1$.

Why are we allowed to do this?

Let WO = Well-Ordering Axiom
PI = Principle of Induction
PSI = Principle of Strong Induction.

If you gave me enough time, I could prove to you that

$$\begin{tikzcd} & \mathrm{WO} \arrow[dl, Leftrightarrow] \arrow[dr, Leftrightarrow] & \\ \mathrm{PI} \arrow[rr, Leftrightarrow] & & \mathrm{PSI} \end{tikzcd}$$

(but you probably wouldn't like it)

They are all logically equivalent. So you can just choose the one that's most convenient in any given situation.

Usually people aren't even explicit about this. They just say "by induction", and leave it to the reader to figure out the details.

Finally, let's write a nice proof.

Theorem: For all $n \geq 0$ we have

$$f_n = \frac{1}{\sqrt{5}}\left[\alpha^{n+2} - \beta^{n+2}\right].$$

Proof by induction: Let

$$P(n) = \text{“} f_n = \frac{1}{\sqrt{5}}\left[\alpha^{n+2} - \beta^{n+2}\right] \text{”}$$

We want to show that $P(n) = T \; \forall n \geq 0$.

Base Cases: We previously checked that $P(0) = P(1) = T$.

Induction Step: Assume for induction that $P(k) = P(k-1) = T$. [We are allowed to assume two cases because we checked two base cases.]
In this case we want to show that $P(k+1) = T$, in other words,

$$f_{k+1} = \frac{1}{\sqrt{5}}\left[\alpha^{k+3} - \beta^{k+3}\right].$$

Indeed, we saw previously that

$$\frac{1}{\sqrt{5}}\left[\alpha^{k+3} - \beta^{k+3}\right]$$

$$= \frac{1}{\sqrt{5}}\left[\alpha^{k+2} - \beta^{k+2}\right] + \frac{1}{\sqrt{5}}\left[\alpha^{k+1} - \beta^{k+1}\right].$$

Since we assumed $P(k) = P(k-1) = T$ this means that

$$\frac{1}{\sqrt{5}}\left[\alpha^{k+3} - \beta^{k+3}\right]$$

$$= f_k + f_{k-1} \quad \text{by assumption}$$

$$= f_{k+1} \quad \text{by the recurrence we proved.}$$

We conclude that $P(k+1) = T$.

By induction we conclude that

$$P(n) = T \quad \forall n \geq 0.$$

//

So the formula is true.

But that still doesn't explain how anyone would guess the formula in the first place.

Q: So how could we <u>guess</u> the formula?

A: Well, this is harder.

The <u>best</u> way to do it is by linear algebra.

We write the recurrence as

$$f_n = f_{n-1} + f_{n-2}$$
$$f_{n-1} = f_{n-1}$$

and then express this via matrices

$$\begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} f_{n-1} \\ f_{n-2} \end{pmatrix}.$$

Now "diagonalize" this matrix.

If you don't know linear algebra, then I suppose we could use Calculus.

The trick is to define the "generating function" for the numbers f_n:

$$F(x) = 1 + 2x + 3x^2 + 5x^3 + 8x^4 + \cdots$$
$$= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \cdots$$

$$F(x) = \sum_{n \geq 0} f_n x^n$$

Turn the recurrence into information about $F(x)$:

$$f_n = f_{n-1} + f_{n-2}$$

$$\sum_{n \geq 2} f_n x^n = \sum_{n \geq 2} (f_{n-1} + f_{n-2}) x^n$$

$$F(x) - (1 + 2x) = \sum_{n \geq 2} f_{n-1} x^n + \sum_{n \geq 2} f_{n-2} x^n$$

$$= x \sum_{n \geq 2} f_{n-1} x^{n-1} + x^2 \sum_{n \geq 2} f_{n-2} x^{n-2}$$

$$= x \sum_{n \geq 1} f_n x^n + x^2 \sum_{n \geq 0} f_n x^n$$

$$= x \left(F(x) - 1 \right) + x^2 F(x).$$

Now solve for $F(x)$:

$$F(x) - (1+2x) = x F(x) - x + x^2 F(x).$$

$$F(x) - x F(x) - x^2 F(x) = 1 + 2x - x.$$

$$F(x) \left(1 - x - x^2 \right) = 1 + x$$

$$F(x) = \frac{1+x}{1-x-x^2}.$$

We conclude that

$$\frac{1+x}{1-x-x^2} = f_0 + f_1 x + f_2 x^2 + \cdots$$

That is, f_n is the coefficient of x^n in the Taylor series for $(1+x)/(1-x-x^2)$ near $x = 0$.

OK, so compute the Taylor series.

How? Well, we'll try to be smart about it. First we observe that

$$1 - x - x^2 = (1-\alpha x)(1-\beta x)$$

where α, β are as before. Then we use the method of partial fractions

$$\frac{1+x}{(1-\alpha x)(1-\beta x)} = \frac{A}{1-\alpha x} + \frac{B}{1-\beta x}$$

$$\frac{1+x}{(1-\alpha x)(1-\beta x)} = \frac{A(1-\beta x) + B(1-\alpha x)}{(1-\alpha x)(1-\beta x)}$$

Equating numerators gives

$$\begin{aligned} 1+x &= A(1-\beta x) + B(1-\alpha x) \\ &= (A+B) + (-\beta A - \alpha B)x. \end{aligned}$$

Equating coefficients gives

$$\left.\begin{aligned} A + B &= 1 \\ -\beta A - \alpha B &= 1 \end{aligned}\right\}$$

Solving this equation gives

$$A = \frac{-\alpha - 1}{\beta - \alpha} = \frac{\alpha^2}{\sqrt{5}}$$

$$B = \frac{\beta + 1}{\beta - \alpha} = -\frac{\beta^2}{\sqrt{5}}$$

Finally we expand using geometric series.

$$F(x) = \frac{1+x}{1-x-x^2} = \frac{\alpha^2}{\sqrt{5}}\frac{1}{(1-\alpha x)} - \frac{\beta^2}{\sqrt{5}}\frac{1}{(1-\beta x)}$$

$$= \frac{\alpha^2}{\sqrt{5}}\left(1 + \alpha x + \alpha^2 x^2 + \alpha^3 x^3 + \cdots\right)$$

$$- \frac{\beta^2}{\sqrt{5}}\left(1 + \beta x + \beta^2 x^2 + \beta^2 x^3 + \cdots\right)$$

$$= \frac{1}{\sqrt{5}}\left((\alpha^2 - \beta^2) + (\alpha^3 - \beta^3)x + (\alpha^4 - \beta^4)x^2 + \cdots\right).$$

In other words, the coefficient of x^n in $F(x)$ is

$$\frac{1}{\sqrt{5}}\left[\alpha^{n+2} - \beta^{n+2}\right].$$

Aren't you glad you remembered how to compute Taylor series?