Proof by Induction (cont'd)

Last time I introduced the basic structure of a proof by induction, and did one basic example. This week will be spent mostly on inductive proofs. We'll start with more examples of regular induction. Then we'll go on to two fancier forms of induction, called strong induction and structural induction.

1 More Simple Inductions

1.1 Divisibility

Definition 1.1 Given two integers x and y, we say x *divides* y, and write $x \mid y$, if there is no remainder on division of y by x. That is, $y = cx$ for some integer c.

Lemma 1.2 $\forall n \in N, n \geq 0(6|n^3 - n)$

We will prove this by induction on n, with base case 0. Thus, $P(n)$ is the predicate $6|n^3 - n$. Base $P(0)$ looks obvious, because $6|0$ by definition. How about the inductive step?

Prove: $\forall n \in N, n \geq 0(6|n^3 - n)$
1. (Base) $6|0^3 - 0$
2. (Inductive step) $\forall n \geq 0(6|n^3 - n \Rightarrow 6|(n+1)^3 - (n+1))$
   1. Fix $n \geq 0$.
   2. Assume $6|n^3 - n$
   3. $6|(n+1)^3 - (n+1)$ — ???
   4. QED — Implication, UG (condensing two steps here)
3. QED — Induction

Now, how to get from 2.2 to 2.3? Since both the expressions have high-order n^3 terms, we can try subtracting. The difference is $((n+1)^3 - (n+1)) - (n^3 - n)$, which works out to $3n^2 + 3n$. If we know that 6 divides this difference, and we are assuming that 6 divides $n^3 - n$, it follows that $6|(n+1)^3 - (n+1)$, which is the sum. That's what we needed.

So the problem reduces to showing $6|3n^2 + 3n$. This factors into $3(n^2 + n)$. But we know that $n^2 + n$ is even, that is, $2|n^2 + n$. If we multiply the expression by 3, then 6 certainly divides the result.

This discussion contained all the ideas needed for the proof. Now we will put it all together in a complete proof.

Proof.

Prove: $\forall n \in N, n \geq 0 (6 | n^3 - n)$
1. (Base) $6 | 0^3 - 0$
2. (Inductive step) $\forall n \geq 0 (6 | n^3 - n \Rightarrow 6 | (n+1)^3 - (n+1))$
    1. Fix $n \geq 0$.
    2. Assume $6 | n^3 - n$
    3. $6 | (n+1)^3 - (n+1)$
        1. $(n+1)^3 - (n+1) = n^3 - n + 3(n^2 + n)$ — Algebra
        2. $n^2 + n$ is even — Proved this last lecture
        3. $2 | n^2 + n$ — Definition of $|$
        4. $6 | 3(n^2 + n)$ — Multiplying both sides by 3 (basic properties of N)
        5. $6 | (n^3 - n) + 3(n^2 + n)$ — Divides both terms (2.2, 2.3.4), so divides sum.
        6. QED — 2.3.1 equality, 2.3.5
    4. QED
3. QED

■

The ideas in this proof are given directly, in the order in which they are *used*. This makes it concise and clear. But this is a different order from the way the ideas arose when we came up with the proof in the first place. By switching the order around, we've lost information about *how we came up with* the proof ideas.

In reading proofs, you will see a tension between trying to provide the reader with the cleanest possible final product and providing intuition about how the proof was developed. Neither extreme is perfect—both kinds of information are useful. When you write proofs, you might want to give both the final product and some discussion of how you arrived at it.

1.2 A string example

Lemma 1.3 There are exactly 2^n different length n strings of 0s and 1s.

Proof. Let $P(n)$ be the given statement.

Prove: $\forall n \geq 0 (P(n))$
1. (Base) $P(0)$ — There's exactly one empty string of 0s and 1s.
2. (Inductive step) $\forall n \geq 0 (P(n) \Rightarrow P(n+1))$
    1. Fix $n \geq 0$.
    2. Assume $P(n)$, that is, there are 2^n length n strings.
    3. $P(n+1)$, that is, there are 2^{n+1} length $n+1$ strings. — Every string of length n can have either a 0 or a 1 attached at the end.
    4. QED — Implication, UG
3. QED — Induction

■

1.3 Fibonacci numbers

The Fibonacci number are interesting numbers that arise, e.g., in biology, where they model some types of growth processes (plants, cells, rabbit populations,...). The Fibonacci numbers are written as F_i, $i = 0, 1, 2, \ldots$. They are defined recursively by:

$$\begin{aligned} &F_0 = 0 \\ &F_1 = 1 \\ &F_i = F_{i-1} + F_{i-2} \text{ for } i \geq 2. \end{aligned}$$

So the sequence starts out $0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$.

The Fibonacci numbers satisfy many cute identities. They provide fun for mathematicians. For example:

Theorem 1.4 $\forall n \geq 0(\Sigma_{i=0}^{n} F_i^2 = F_n F_{n+1})$

Example: $n = 4$:
$0^2 + 1^2 + 1^2 + 2^2 + 3^2 = 15 = 3 \cdot 5$.
Let's try a proof by induction. The theorem statement suggests trying it with $P(n)$ defined as:

$$\sum_{i=0}^{n} F_i^2 = F_n F_{n+1}$$

Prove: $\forall n \geq 0(\Sigma_{i=0}^{n} F_i^2 = F_n F_{n+1})$
1. (Base) $\Sigma_{i=0}^{0} F_i^2 = F_0 F_1$
2. (Inductive step) $\forall n \geq 0(\Sigma_{i=0}^{n} F_i^2 = F_n F_{n+1} \Rightarrow \Sigma_{i=0}^{n+1} F_i^2 = F_{n+1} F_{n+2})$
???
3. QED Induction

Now we stare at the gap between $P(n)$ and $P(n+1)$. $P(n+1)$ is given by a summation that's obtained from that for $P(n)$ by adding one term; this suggests that, once again, we subtract. The difference is just the term F_{n+1}^2. Now, we are assuming that the original $P(n)$ summation totals $F_n F_{n+1}$ and want to show that the new $P(n+1)$ summation totals $F_{n+1} F_{n+2}$. So we would *like* the difference to be

$$F_{n+1} F_{n+2} - F_n F_{n+1}$$

So, the actual difference is F_{n+1}^2 and the difference we want is $F_{n+1} F_{n+2} - F_n F_{n+1}$. Are these the same? We want to check that:

$$F_{n+1}^2 = F_{n+1} F_{n+2} - F_n F_{n+1}$$

But this is true, because it is really the Fibonacci definition in disguise: to see this, divide by F_{n+1}. Here's the complete proof:

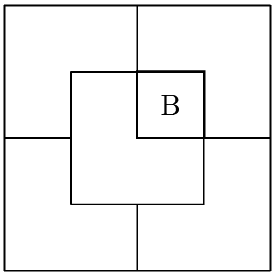

Figure 1: A legal tiling of a 4x4 courtyard. The B marks Bill.

Prove: $\forall n \geq 0(\Sigma_{i=0}^{n} F_i^2 = F_n F_{n+1})$
1. (Base) $\Sigma_{i=0}^{0} F_i^2 = F_0 F_1$ — Both sides are 0.
2. (Inductive step) $\forall n \geq 0(\Sigma_{i=0}^{n} F_i^2 = F_n F_{n+1} \Rightarrow \Sigma_{i=0}^{n+1} F_i^2 = F_{n+1} F_{n+2})$
   1. Fix $n \geq 0$.
   2. Assume $\Sigma_{i=0}^{n} F_i^2 = F_n F_{n+1}$
   3. $\Sigma_{i=0}^{n+1} F_i^2 = F_{n+1} F_{n+2}$
      1. $\Sigma_{i=0}^{n+1} F_i^2 = \Sigma_{i=0}^{n} F_i^2 + F_{n+1}^2$ — Summation has one extra term
      2. $\Sigma_{i=0}^{n} F_i^2 + F_{n+1}^2 = F_n F_{n+1} + F_{n+1}^2$ — Inductive hypothesis (2.2)
      3. $F_n F_{n+1} + F_{n+1}^2 = F_{n+1}(F_n + F_{n+1})$ — Algebra
      4. $F_{n+1}(F_n + F_{n+1}) = F_{n+1} F_{n+2}$ — Fibonacci definition
      5. QED — Combining the equations
   4. QED — Implication, UG
3. QED — Induction

2 Tiling

Our next proof illustrates some new ideas:

- Sometime you need to strengthen inductive hypothesis in order to prove it.
- Sometime induction helps finding a construction, not just do a proof

The new CS building currently under construction will cost about \$140 million. Money has come from many donors, including Bill Gates. Donors get something in return, e.g., something named after them. What Bill G. wants is one of the buildings named after him, plus a statue of himself in the middle of the courtyard.

The planned courtyard consists of $2^n \times 2^n$ squares, for some $n \geq 1$. (We don't yet know how big n is). The architect, Frank Gehry, wants to cover most of this with L-shaped tiles, each covering three squares. But one of the four center squares will be left empty, for the statue. Can this be done? If so, how (we want a general solution, for all values of n).

Example: $n = 2$

Can we prove what we want by induction? For $P(n)$, let's try:
For any $2^n \times 2^n$ courtyard, and any particular central square, $\exists$ a tiling of the courtyard with exactly that square left untiled.

Proof. *(doomed attempt)* In the base case: $n = 1$, we can use just one tile. In the inductive step, we try to produce a tiling of a $2^{n+1} \times 2^{n+1}$ courtyard with one center square blank. We can assume tilings of any $2^n \times 2^n$ courtyard with any center square blank. We might think of subdividing into four $2^n \times 2^n$ sub-courtyards. But it doesn't seem to help to be able to tile those with centers left open... ■

Here we've hit the first case where just trying to prove the statement directly by induction doesn't work. The solution may be surprising: Try to prove a *stronger* theorem that implies the one we want.

Isn't that harder?

Actually, strengthening a statement to be proved by induction often makes the proof *easier*. The reason is that, although we have to prove a stronger $P(n+1)$, we also can rely on a stronger $P(n)$.

Here, let's redefine $P(n)$ to be the predicate that says, for *every* square in a $2^n \times 2^n$ courtyard, we can tile the rest. Stronger. But now $P(n) \Rightarrow P(n+1)$ is easier. And the theorem we wanted originally is just a special case.

Proof. Induction. The base, $P(1)$, is as before. For the inductive step, $n \geq 1$, start with an arbitrary $2^{n+1} \times 2^{n+1}$ courtyard with an arbitrary square to leave blank. Let's try to tile this, assuming tilings of any $2^n \times 2^n$ courtyard with *any* square blank.

Again, divide the $2^{n+1} \times 2^{n+1}$ courtyard into four $2^n \times 2^n$ quadrants. One will contain the square that must be left blank; it can be tiled by inductive hypothesis.

Next, put one tile in the center, covering one square in each of the other 3 quadrants. Now use the inductive hypothesis three more times to tile the rest of the 3 quads. ■

You should make sure you understand the logical structure of this proof.

This proof provides a tiling method, not just existence proof. And it gives a stronger result than we needed.

3 Geometry

Definition 3.1 A convex polygon is a polygon such that any straight line between any two vertices doesn't leave the polygon

$P(n)$: The sum of the interior angles in any n-sided convex polygon is exactly $(n-2)180$ degrees.
Prove: $\forall n \geq 3$ (The sum of the interior angles in any n-sided convex polygon is exactly $(n-2)180$ degrees.)

1. (Base) Sum of angles in any triangle is 180. Basic fact from geometry
2. (Inductive step) $\forall n \geq 3 (P(n) \Rightarrow P(n+1))$
    1. Fix $n \geq 3$.
    2. Assume sum of angles of any n-sided convex poly is $(n-2)180$.
    3. Sum of angles of any $n+1$-sided convex poly is $(n-1)180$.
        1. Fix any $n+1$-vertex convex poly X, say with vertices $x_1, x_2, \ldots, x_{n+1}$
        2. Let Y be the poly with vertices $x_1, x_2, \ldots, x_n$ (cutting out one vertex).
        3. Y is a convex poly with at least 3 vertices.
        4. Sum of interior angles of Y is $(n-2)180$.

Inductive hypothesis (2.2)

5. Sum of interior angles of triangle $T = x_n, x_{n+1}, x_1$ is 180.

Basic fact from geometry

6. Sum of angles in X = sum in Y + sum in T, $= (n-2)180 + 180 = (n-1)180$.

Basic geometry, arithmetic.

7. QED — UG

4. QED — Implication, UG

3. QED — Induction

(UG is used to conclude something about all polynomials from what we showed for any particular one.)

4 Double Induction

Here's a trickier use of induction, used twice, in a nested way, in the same proof.

Define a function of two N variables recursively as follows:
$f(0,k) = 1$ for all $k \geq 0$.
$f(n,0) = 1$ for all $n \geq 0$.

For $n, k \geq 0:$
$f(n+1, k+1) = f(n, k+1) + f(n+1, k)$.

Why does this define a function? We can see by looking at a table. The first two rules fill in the first row and column, respectively. For each other entry, you obtain the value by adding bottom and left neighbors. It is left to the reader to see that this defines a unique function, that is, fills in all the spaces, in exactly one way.

4	1	5	15	35	70
3	1	4	10	20	35
2	1	3	6	10	15
1	1	2	3	4	5
0	1	1	1	1	1
	0	1	2	3	4

We will see these numbers later in the term. For now, notice a formula (which we pull out of thin air):

$$f(n,k) = \frac{(n+k)!}{n!k!}.$$

Here we are using the factorial function (written "!"):

$$0! = 1$$
$$1! = 1$$
$$n! = n(n-1)\dots 1$$

Example:
$f(3,4) = \frac{7!}{3!4!} = \frac{7.6.5.4.3.2.1}{3.2.1.4.3.2.1} = 35.$

Lemma 4.1 $\forall n, k \in N(f(n,k) = \frac{(n+k)!}{n!k!})$.

We can prove this by induction. But there are two variables, n and k. So, we will do the proof in 2 levels. The main strategy is by induction on n. And for each particular n, we work by induction on k. We are doing induction inside an induction.

Let's break up the statement to make the two levels clearer:

Lemma 4.2 $\forall n(\forall k(f(n,k) = \frac{(n+k)!}{n!k!}))$

Define $Q(n,k)$ to be the predicate $f(n,k) = \frac{(n+k)!}{n!k!}$. $Q(n,k)$ says that the value in position (n,k) is correct (satisfies the formula). Define $P(n)$ to be $\forall k(Q(n,k))$, that is, $\forall k(f(n,k) = \frac{(n+k)!}{n!k!})$. $P(n)$ means that all the values in row n are correct.

We use the induction pattern:

Prove: $\forall n \geq 0(P(n))$	
1. (Base) $P(0)$	
2. (Inductive step) $\forall n \geq 0(P(n) \Rightarrow P(n+1))$	
3. QED	Induction

Expanding this pattern:

Prove: $\forall n \geq 0(P(n))$	
1. (Base) $P(0)$	
1. $\forall k(f(0,k) = \frac{(0+k)!}{0!k!})$	Both sides are 1
2. QED	Definition of $P(0)$
2. (Inductive step) $\forall n \geq 0(P(n) \Rightarrow P(n+1))$	
1. Fix $n \geq 0$.	
2. Assume $P(n)$, that is, row n is correct.	
3. $P(n+1)$, that is, row $n+1$ is correct.	???
4. QED	Implication, UG
3. QED	Induction

Now, how to prove 3? It involves saying something about the whole row $n+1$. We use induction to handle all the elements in this row one at a time. Our goal 3 can be rewritten, using the definition of P in terms of Q. Note that this is all talking just about row $n+1$.

3. $P(n+1)$	
1. $\forall k(Q(n+1,k))$	
1. (Base) $Q(n+1,0)$	
2. (Inductive step) $\forall k \geq 0(Q(n+1,k) \Rightarrow Q(n+1,k+1))$.	
3. QED	Induction
2. QED	Definition of $P(n+1)$

The base case for the inner induction follows by expanding the definition of $Q(n+1,0)$:

1. (Base) $Q(n+1,0)$
   1. $f(n+1,0) = \frac{(n+1+0)!}{n+1!0!}$ — Both sides are 1
   2. QED — Definition of $Q(n+1)$

The inductive step involves some algebra:

2. (Inductive step) $\forall k \geq 0(Q(n+1,k) \Rightarrow Q(n+1,k+1))$.
   1. Fix $k \geq 0$.
   2. Assume $Q(n+1,k)$.
   3. $Q(n+1,k+1)$
      1. $f(n+1,k+1) = f(n,k+1) + f(n+1,k)$ — Definition of $f(n+1,k+1)$
      2. $f(n+1,k) = \frac{(n+1+k)!}{(n+1)!k!}$ — Inductive hypothesis 2.3.1.2.2, def. of $Q(n+1,k)$.
      3. $f(n,k+1) = \frac{(n+k+1)!}{n!(k+1)!}$ — Inductive hypothesis 2.2, def. of $P(n,k+1)$.
      4. $f(n+1,k+1) = \frac{(n+k+1)!}{n!(k+1)!} + \frac{(n+1+k)!}{(n+1)!k!} = \frac{(n+1+k+1)!}{(n+1)!k+1!}$ — Combining equations, algebra
      5. QED — Definition of $Q(n+1,k+1)$
   4. QED — Induction

The inner inductive hypothesis is invoked to get info about the previous element in the same row, $n+1$. The outer inductive hypothesis is then invoked to get info about element $k+1$ of the previous row. (The proof uses UI.)

5 Strong induction

Now we explore a more-powerful-seeming variant on the ordinary induction principle. Recall ordinary induction:

Prove: $\forall n \geq 0(P(n))$
1. (Base) $P(0)$
2. (Inductive step) $\forall n \geq 0(P(n) \Rightarrow P(n+1))$
3. QED — Induction

Strong induction gives alternative way to prove the same kind of statements:

Prove: $\forall n \geq 0(P(n))$
1. (Base) $P(0)$
2. (Inductive step) $\forall n \geq 0[(\forall i, 0 \leq i \leq n(P(n))) \Rightarrow P(n+1)]$
3. QED — Strong induction

The implication within the inductive step is easier to show than it is for ordinary induction, because now in order to prove $P(n+1)$, we can assume all of the hypotheses $P(0), P(1), P(2), \dots, P(n)$, not just $P(n)$. This is written like a new deduction rule. We can also write it as an axiom:

$$[P(0) \wedge \forall n \geq 0[(\forall i, 0 \leq i \leq n(P(n))) \Rightarrow P(n+1)]] \Rightarrow \forall n(P(n)).$$

Why does this method work? Well, we want to prove for $0, 1, 2, \dots$. We get $P(0)$ for free. Then we know $P(0) \Rightarrow P(1)$, which tells us $P(1)$ (modus ponens). Then we know $P(0) \wedge P(1) \Rightarrow P(2)$, which, since we know $P(0) \wedge P(1)$, tells us $P(2)$. Etc.

Of course, we can do the same thing starting from any k, not just 0:

Prove: $\forall n \geq k(P(n))$
1. (Base) $P(k)$
2. (Inductive step) $\forall n \geq k[(\forall i, k \leq i \leq n(P(n))) \Rightarrow P(n+1)]$
3. QED — Strong induction

Let's do some strong induction proofs.

5.1 Blocks and towers

Given an unlimited number of blocks of heights 3 and 7, what height towers can be built?

Try some possible heights:
1: no
2: no
3: yes, 3
4: no
5: no
6: 3+3
7: 7
8: no
9: 3+3+3
10: 3 + 7
11: no
12: 3+3+3+3
13: 7+3+3
14: 7+7
15: 3+3+3+3+3
16: 7+3+3+3

From this point on, can we make all larger height towers?
Define $P(n)$ to be "we can build a tower of height n". We prove this by strong induction:

Prove: $\forall n \geq 12(P(n))$
1. (Base) $P(12)$ — Use 3+3+3+3
2. (Inductive step) $\forall n \geq 12[(\forall i, 12 \leq i \leq n(P(n))) \Rightarrow P(n+1)]$
3. QED — Strong induction

Here's the idea for the inductive step. We can build a tower of height $n-2$, by inductive hypothesis, then add one 3-block. That is, use $P(n-2)$ to show $P(n+1)$. But there's a catch: this works only if $n-2 \geq 12$, i.e., $n \geq 14$. (We can only assume P for arguments ≥ 12.)

For $n = 12, 13$, need to make special arguments.

So, we really have an argument by cases, within the inductive step:

2. (Inductive step) $\forall n \geq 12[(\forall i, 12 \leq i \leq n(P(n))) \Rightarrow P(n+1)]$	
1. Fix $n \geq 12$.	
2. $(\forall i, 12 \leq i \leq n(P(n))) \Rightarrow P(n+1)$	
1. Assume $\forall i, 12 \leq i \leq n(P(n)$	
2. $P(n+1))$	
1. $n = 12 \Rightarrow P(n+1)$	Use 7+3+3
2. $n = 13 \Rightarrow P(n+1)$	Use 7+7
3. $n \geq 14 \Rightarrow P(n+1)$	???
4. QED	Cases
3. QED	Implication
3. QED	UG

The first two special cases are easy—we've already done them. The last case is the one covered by the idea sketched earlier.

3. $n \geq 14 \Rightarrow P(n+1)$	
1. Assume $n \geq 14$.	
2. $P(n-2)$	By inductive hypothesis 2.2.1 and the fact that $n-2 \geq 12$
3. $P(n+1)$	Add one block to the tower from the previous step.
4. QED	Implication

Look at the logical structure. I wrote this as a single base case (for 12) and inductive step, where the inductive step breaks down into two special cases (for 13 and 14) plus the rest. I could also formulate a variant on the proof rule:

Prove: $\forall n \geq 12(P(n))$	
1. (Base) $P(12)$	
2. (Base) $P(13)$	
3. (Base) $P(14)$	
4. (Inductive step) $\forall n \geq 14[(\forall i, 12 \leq i \leq n(P(n))) \Rightarrow P(n+1)]$	
3. QED	Very specialized strong induction

In examples like these, you must be careful to consider all the needed base (or special) cases. Otherwise, you might "prove" false theorems, e.g., that we can build all towers of size ≥ 3:

Prove: $\forall n \geq 3(P(n))$	
1. (Base) $P(3)$	
2. (Inductive step) $\forall n \geq 3[(\forall i, 3 \leq i \leq n(P(n))) \Rightarrow P(n+1)]$	
3. QED	Strong induction

If we try to mimic the previous proof for this situation, we find we can't make the jump to 4 or 5.

5.2 Nim

The game of Nim is defined as follows: Some positive number of sticks are placed on the ground. Two players take turns removing one, two, or three sticks. The player to remove the last stick loses.

Theorem 5.1 The first player loses if the number of sticks, n, is $4k+1$ for some k, and wins (if he plays optimally) otherwise.

We can formalize this by defining a strategy as a rule for how many sticks to remove when there are n left. We then show that if $n = 4k+1$, then player 2 has a strategy that will force a win for him, otherwise, player 1 has a strategy that will force a win for him.

Proof. By strong induction. Suppose the theorem is true for numbers less than n, show that it is true for n. So we want to show that if $n = 4k+1$ then first player loses, otherwise if $n = 4k$, $4k+2$, or $4k+3$, then the first player wins. (We'll see later why this exhausts all possible cases for n)

Base case: $n = 1$. The first player has no choice but to remove 1 stick and lose.

For the inductive step, there are four cases:

- $n = 4k+1$: show that the first player loses.

  We've already handled the base case ($n = 1$) so we can assume $n \geq 5$. Consider what the first player might do to win: he can choose to remove 1, 2 or 3 sticks. If he removes one stick, the remaining number of sticks is $n-1 = 4k$. By strong induction, the player who plays at this point should win. So the player who played first will lose.

  Similarly, if the first player removes two sticks, the remaining amount is $4(k-1)+3$. He, again, loses by the same reasoning.

  And again by removing 3 sticks, he loses.

  So however the first player moves, he loses.

- $n = 4k$: show that the first player can win.

  Have first player remove 3 sticks: the second player then sees $4(k-1)+1$ sticks, and loses, by the strong inductive hypothesis.

- $n = 4k+2$: show that the first player can win.

  Similar to the previous case when the first player removes one stick.

- $n = 4k+3$: show that the first player can win.

  Again similar to the previous case when the first player removes two sticks.

∎

5.3 Fibonacci examples

5.3.1 Another false theorem

Here is another false "theorem". The fallacy is like the blocks example—we don't have enough base cases.

False Theorem 1 All Fibonacci numbers are even.

We try strong induction, where $P(n)$ is defined to be "F_n is even."

Prove: $\forall n \geq 0(P(n))$
1. (Base) $P(0)$
   $F_0 = 0$, which is even.
2. (Inductive step) $\forall n \geq 0[(\forall i, 0 \leq i \leq n(P(n))) \Rightarrow P(n+1)]$
   ???
3. QED — Strong induction

The inductive step is supposed to prove that F_{n+1} is even, using the fact that all smaller Fibonacci numbers are even. The idea to express F_{n+1} as usual, as $F_{n-1} + F_n$. Then use the strong inductive hypothesis to say that F_{n-1} and F_n are both even. The sum is therefore also even.
Error?
We Proved: $P(0)$
$P(0) \wedge P(1) \Rightarrow P(2)$
$P(1) \wedge P(2) \Rightarrow P(3)$
etc. But we never proved $P(1)$.

5.3.2 A lower bound

Here's a correct proof about Fibonacci numbers. It's a lower bound on their values.

Lemma 5.2 $\forall n \geq 2(F_n \geq (\frac{3}{2})^{n-2})$

Proof. Use strong induction. Let $P(n) = F_n \geq (\frac{3}{2})^{n-2}$

Prove: $\forall n \geq 2(P(n))$
1. (Base) $P(2)$ — $F_2 = 1 = (\frac{3}{2})^0$
2. (Base) $P(3)$ — $F_3 = 2 \geq (\frac{3}{2})^1$
3. (Inductive step) $\forall n \geq 3[(\forall i, 2 \leq i \leq n(P(i))) \Rightarrow P(n+1)]$
    1. Fix $n \geq 3$
    2. Assume $\forall i, 2 \leq i \leq n(P(i))$
    3. $P(n+1)$ — ???
    4. QED — Implication, UG
4. QED — Strong induction

Now in proving the ??? we are only worrying about $n \geq 3$ and we may assume the inequality for all i from 2 up to n, inclusive. Because of the way Fibonacci numbers are defined, it turns out that the ones we need are just n and $n-1$. Those are in the range for which we can assume the property.

3. $P(n+1)$
   1. $F_n \geq (\frac{3}{2})^{n-2}$ — Inductive hypothesis 3.2
   2. $F_{n-1} \geq (\frac{3}{2})^{n-3}$ — Inductive hypothesis 3.2
   3. $F_{n+1} = F_n + F_{n-1}$ — Definition
   4. $F_{n+1} \geq (\frac{3}{2})^{n-2} + (\frac{3}{2})^{n-3}$ — Plug the inequalities into the equation
   5. QED — Algebra
      1. $\frac{3}{2} + 1 \geq (\frac{3}{2})^2$ — Arithmetic
      2. $(\frac{3}{2})^{n-2} + (\frac{3}{2})^{n-3} \geq (\frac{3}{2})^{n-1}$ — Algebra
      3. $F_{n+1} \geq (\frac{3}{2})^{n-1}$ — Algebra (3.3.4 and 3.3.5.2)
      4. QED — Definition of $P(n+1)$

■

5.4 Prime Factorization

Recall that a prime is a number not evenly divisible by any number but itself and one. $2, 3, 5, 7, 11, \ldots$ are primes. $4, 6, 8, 9, 10, 12, \ldots$ are not. They are composites.

Notice, however, that each composite can be broken down (factored) into primes. E.g., $12 = 2 \times 2 \times 3$. This is not a coincidence.

Theorem 5.3 Every natural number ≥ 2 can be written as the product of one or more primes.

Proof. We use strong induction, starting from 2, where $P(n)$ is the predicate "n can be written as the product of one or more primes".

Prove: $\forall n \geq 2(P(n))$
1. $P(2)$ — Use 2 itself
2. $\forall n \geq 2[(\forall i, 2 \leq i \leq n)(P(i)) \Rightarrow P(n)]$
   1. Fix $n \geq 2$
   2. Assume $\forall i, 2 \leq i \leq n(P(i))$, that is, all numbers up to and including n can be factored into primes
   3. $P(n+1)$, that is, $n+1$ can be factored into primes. — ???
   4. QED — Implication, UG
3. QED — Strong induction

The argument about factoring $n+1$ breaks down into cases, depending on whether or not $n+1$ itself is prime:

3. $P(n+1)$, that is, $n+1$ can be factored into primes.
   1. If $n+1$ is prime, then $n+1$ can be factored into primes. — Use $n+1$ itself
   2. If $n+1$ is not prime, then $n+1$ can be factored into primes.
      1. Assume $n+1$ is not prime.

2. $n+1$ can be written as $a \times b$, where $1 < a, b < n+1$	Definition of "prime"
3. a can be factored into primes.	Strong inductive hypothesis (2.2)
4. b can be factored into primes.	Strong inductive hypothesis (2.2)
5. $n+1$ can be factored into primes.	Use all the factors from a and b.
6. QED	Implication
3. QED	Cases

We can do the above a little more carefully. If a is written as a product $2^{a_2}3^{a_3}5^{a_5}\cdots$ and b is written as a product $2^{b_2}3^{b_3}5^{b_5}\cdots$ then $n+1 = ab$ is written as $2^{a_2+b_2}3^{a_3+b_3}5^{a_5+b_5}\cdots$. We just add the number of occurrences of each separate prime factor. ■

Example 5.4 A factorization of 144 can be obtained by noticing that $144 = 8 \times 18$ (among other possibilities). 8 can be written as 2^3, and 18 as 2×3^2. So, write 144 as $2^{3+1}3^2$, or $2^4 3^2$.