Example Prove $(\forall n \in \mathbb{N})\ (n+1)^2 = n^2 + 2n + 1$

Proof Let n be any natural number. Then

$$
\begin{aligned}
(n+1)^2 &= (n+1)(n+1) \\
&= (n+1)\cdot n + (n+1)\cdot 1 && (\textit{distributive law for arithmetic in } \mathbb{N}) \\
&= n\cdot n \ + \ 1\cdot n + \ n\cdot 1 + 1\cdot 1 \\
&= n^2 \ + \ n\cdot 1 \ + \ n\cdot 1 \ + \ 1 && \text{because}\_\_\_\_\_ \\
&= n^2 + n\cdot(1+1) \ + \ 1 && \text{because}\_\_\_\_\_ \\
&= n^2 + n\cdot 2 + 1 && \text{because}\_\_\_\_\_ \\
&= n^2 + 2n + 1 \qquad \bullet
\end{aligned}
$$

A proof of a statement of the form $(\forall n \in \mathbb{N})\ P(n)$ without using induction ? ? ?

Yes and no. The proof depends only on properties of arithmetic such as the commutative law for multiplication, the distributive law, ... However, why are those true. It turns out (when we construct the system of natural numbers from set theory) that we need to prove these properties of arithmetic, and the proofs <u>*use induction.*</u>

If you go all the way down to the foundations of the natural number system, $\mathbb{N}$, it turns out that proving <u>*every*</u> *statement of the form $(\forall n \in \mathbb{N})\ P(n)$ depends in some way on induction. At the most basic level, it is the* <u>*only*</u> *tool for proving assertions about "all $n \in \mathbb{N}$."*

Example What is <u>wrong</u> with the following "proof" that $(\forall n \in \mathbb{N}) \ \sum_{i=1}^{n} 2i = n^2 + n + 7$
(or, stated more informally, that: $(\forall n \in \mathbb{N}) \quad 2 + 4 + ... + 2n = n^2 + n + 7$) ?

Proof $P(n)$ is the statement: $\sum_{i=1}^{n} 2i = n^2 + n + 7$
Assume that $P(n)$ is true for some particular natural number $n = k$: for this k,
$\sum_{i=1}^{k} 2i = k^2 + k + 7.$

(*Now we need to prove that* $P(k+1)$ *is true:* $\sum_{i=1}^{k+1} 2i = (k+1)^2 + (k+1) + 7$)

$$\sum_{i=1}^{k+1} 2i = \sum_{i=1}^{k} 2i + 2(k+1) = (k^2 + k + 7) + 2(k+1) = k^2 + 3k + 9$$

$\uparrow$
why?

$$= (k^2 + 2k + 1) + k + 8 = (k+1)^2 + (k+1) + 7, \qquad \text{so } P(k+1) \text{ is true.}$$

By PMI we can conclude that $(\forall n \in \mathbb{N}) \sum_{i=1}^{n} 2i = n^2 + n + 7.$ •

The statement $(\forall n \in \mathbb{N}) \ \sum_{i=1}^{n} 2i = n^2 + n + 7$ *is* <u>*false*</u> *(test it for* $n = 1$*) so there* <u>*must*</u> *be something wrong with the "proof." The base case for the induction* $(n = 1)$ *was never checked. There are no errors in the algebra, above: if* $P(1)$ *were true, the rest of the argument, as written, would is correct.*

The following example gives a different proof of a result from the last lecture. Notice the difference in the approach; but, equally important <u>notice the similarities</u> in the algebra that comes up. You can decide whether you prefer this argument to the one using PMI in Example 1.

Example Use WOP to prove: $(\forall n \in \mathbb{N})\, P(n)$, where $P(n)$ is the statement: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Proof Let $A = \{n \in \mathbb{N} : \ P(n)$ is <u>false</u>$\}$.

(*To complete the proof, <u>we want to show that</u>* $A = \emptyset$. *We argue by contradiction.*)

<u>Assume</u> $A \neq \emptyset$. Then, by WOP, there must be a <u>smallest k in A</u>: that is,

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2} \text{ is } \underline{\text{false}} \ \ (*) \quad \underline{\text{and}}$$

$$P(n) \text{ is true for natural numbers } n \text{ smaller than } k.$$

Since $\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$ is <u>true</u>, we know $k \neq 1$, so $k > 1$. Therefore $n = k - 1$ is still a natural number and smaller than k, so $P(k-1)$ must be true:

$$\sum_{i=1}^{k-1} i = \frac{(k-1)((k-1)+1)}{2} = \frac{(k-1)(k)}{2} \qquad \text{is } \underline{\text{true}}. \quad (**)$$

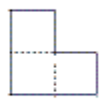
Then adding k to both sides of (**) gives that $\sum_{i=1}^{k-1} i + k = \frac{(k-1)(k)}{2} + k$ is <u>true</u>.

But this equation (*do the algebra!*) simplifies to $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ – which contradicts $(*)$.

Since the assumption that $A \neq \emptyset$ leads to a contradiction, it must be that $A = \emptyset$; in other words,

$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ is true for all $n \in \mathbb{N}$. •

Example A <u>tromino</u> consists of three 1×1 squares, arranged in the shape af an " L "



Prove that the following statement is true for all $n \in \mathbb{N}$.

$P(n)$: Remove <u>one</u> square from a $2^n \times 2^n$ checkerboard. (A *standard checkerboard has* $n = 3$.) The remaining squares can be tiled (= "completely covered, with no overlaps") using trominos.

Proof If $n = 1$ (a 2×2 checkerboard) and one square is removed, the remaining squares form one tromino, so the remainder can be tiled (with one tromino). So $P(1)$ is true.

Suppose $P(n)$ is true for some particular value $k = n$ – that is, assume the statement is true for a $2^k \times 2^k$ checkerboard. (*We now need to prove that* $P(k+1)$ *must be true.*)

(*<u>Draw a picture to help you visualize each step!</u>*) Consider a $2^{k+1} \times 2^{k+1}$ checkerboard. Call it S. Subdivide it vertically and horizontally into 4 square sub-checkerboards, each of size $2^k \times 2^k$. For convenience, number these as S_1, S_2, S_3, S_4.

Remove a square from the larger board and call the remaining figure D. The square removed was in of S_1, S_2, S_3, S_4 (*it doesn't matter which one – let's say it was in* S_1).

i) By the induction assumption, the remainder of S_1, after that one square is removed, can be tiled with trominoes.

ii) Place a tromino at the center where S_2, S_3, S_4 meet. This tromino covers one square from each of S_2, S_3, S_4. By the induction assumption, the remaining squares in each (separately) of S_2, S_3, S_4 can be tiled with trominoes.

In this way, all of D is tiled with trominoes, so $P(k+1)$ is true.

Therefore, by PMI, $P(n)$ is true for all $n \in \mathbb{N}$. •

Example Prove $2^n > n^2$ if $n \geq 5$

Proof (*Here,* $P(n)$ *is the statement* $2^n > n^2$. *We use the Generalized PMI to prove* $P(n)$ *is true for all* $n \geq 5$.)

i) $2^5 > 5^2$, so $P(n)$ is true for $n = 5$.

ii) Suppose $P(n)$ is true for some value $n = k$, where $k \geq 5$.

(*Now we need to show that* $P(k+1)$ *is true:* $2^{k+1} > (k+1)^2$

$$2^{k+1} = 2(2^k) \underset{\substack{\uparrow \\ \textit{why?}}}{>} 2k^2 = k^2 + k^2 = k^2 + k \cdot k \underset{\substack{\uparrow \\ \textit{why?}}}{\geq} k^2 + 5k = k^2 + 2k + (3k+1)$$

$> k^2 + 2k + 1 = (k+1)^2$. Therefore $P(k+1)$ is true.

By PMI, $P(n)$ is true for all $n \geq 5$. •

Example

Let $\Omega(n)$ denote the number of (not necessarily distinct) prime factors of n. If n is prime, we agree that $\Omega(n) = 1$.

$$\Omega(5) = 1$$

$12 = 2 \cdot 2 \cdot 3$, so $\Omega(12) = 3$. Notice that $3 \leq \log_2(12) \approx 3.5850$

Theorem For a natural number n larger than 1: $\Omega(n) \leq \log_2(n)$

$P(n)$ is the statement $\Omega(n) \leq \log_2(n)$. *We want to prove that $P(jn)$ is true for $n \geq 2$.* We will use GPCI.

Proof $\Omega(2) = 1 \leq \log_2(2) = 1$. So $P(2)$ is true.

Suppose k is some particular natural number, where $k > 2$. Assume that $P(n)$ is true for all $n < k$. (*We need to show, using this assumption, that $P(k)$ is true.*) We look at two cases:

<u>If k is prime</u>, then $\Omega(k) = 1 \leq \log_2(k)$ (*since $k > 2$, $log_2(k) > log_2 2 = 1$*)

<u>If k is not prime</u> then (since $k > 2$) we can write $k = pq$ where $1 < p < k$ and $1 < q < k$. Then

$$\Omega(k) = \Omega(pq) \underset{\substack{\uparrow \\ \textit{why?}}}{=} \Omega(p) + \Omega(q) \underset{\substack{\uparrow \\ \textit{by the induction hypothesis}}}{\leq} \log_2(p) + \log_2(q) \overset{\substack{\textit{basic property of logatirhms} \\ \downarrow}}{=} \log_2(pq) = \log_2(k).$$

So $P(k)$ is true.

By GPCI, $(\forall n \in \mathbb{N})\, P(n)$ is true. •

Example Suppose an ATM machine can only give out \$2 bills and \$5 bills (you key in the amount you want, and it figures out how many \$2 bills and \$5 bills to give you).

Prove that the ATM is able to give you \$ n for any $n \geq 4$.

$P(n)$ is the statement: the ATM can dispense \$$n$. We want to prove $P(n)$ is true for all $n \geq 4$.

Exercise