Mathematical Induction

Joseph R. Mileti

February 4, 2015

1 Induction

Suppose that we want to prove that a certain statement is true for all natural numbers. In other words, we want to do the following:

- Prove that the statement is true for 0.
- Prove that the statement is true for 1.
- Prove that the statement is true for 2.
- Prove that the statement is true for 3.
- ....

Of course, since there are infinitely many natural numbers, going through each one in turn does not work because we will never handle them all this way. How can we get around this? Suppose that when we examine the first few proofs above that they look the same except that we replace 0 by 1 everywhere, or 0 by 2 everywhere, etc. In this case, one is tempted to say that "the pattern continues" or something similar, but that is not convincing because we can't be sure that the pattern does not break down when we reach 5413. However, one way to see that the "the pattern continues" and handle all of the infinitely many possibilities at once is to take an arbitrary natural number n, and prove that the statement is true for n using *only* the fact that n is a natural number (but *not* any particular natural number).

The method of taking an arbitrary $n \in \mathbb{N}$ and proving that the statement is true for n is that standard way of proving a statement involving a "for all" quantifier. This technique also works to prove that a statement is true for all rational numbers, all real numbers, all finite sequences of 0's and 1's, etc., as long as we take an *arbitrary* such object. However, there is a different method one can use to prove that every natural number has a certain property, and this one does not carry over to other situations such as the real numbers. The key fact is that the natural numbers start with 0 and proceed in discrete steps forward. Consider what would if we can prove each of the following:

- Prove that the statement is true for 0.
- Prove that if the statement is true for 0, then the statement is true for 1.
- Prove that if the statement is true for 1, then the statement is true for 2.
- Prove that if the statement is true for 2, then the statement is true for 3.
- ....

Suppose that we are successful in doing this. From the first line, we then know that the statement is true for 0. Since we now know that it's true for 0, we can use the second line to conclude that the statement is true for 1. Since we now know that it's true for 1, we can use the second line to conclude that the statement is true for 2. And so on. In the end, we are able to conclude that the statement is true for all natural numbers.

Let's examine this situation more closely. On the fact of it, each line looks more complicated than the corresponding lines for proving a theorem directly. However, the key fact is that from the second line onward, we now have an additional assumption! Thus, instead of proving that the statement is true for 3 without any help, we can now use the assumption that the statement is true for 2 in that argument. Extra assumptions are always welcome because we have more that we can use in the actual argument.

Of course, as in our discussion at the beginning of this section, we can't hope to prove each of these infinitely many things one at a time. In an ideal world, the arguments from the second line onward all look exactly the same with the exception of replacing the number involved. Thus, the idea is to prove the following.

- Prove that the statement is true for 0.
- Prove that if the statement is true for n, then the statement is true for $n + 1$.

Notice that for the second line, we would need to prove that it is true for an arbitrary $n \in \mathbb{N}$, just like we would have to in a direct argument. An argument using this method is called a proof by (mathematical) *induction*, and it is an extremely useful and common technique in discrete mathematics. We now state this approach formally in terms of sets, which allows us to bypass the vague notion of "statement" that we used above.

Fact 1.1 (Principle of Mathematical Induction on $\mathbb{N}$)**.** *Let $X \subseteq \mathbb{N}$. Suppose that the following are true:*

- $0 \in X$ *(the* base case*)*
- $n + 1 \in X$ *whenever* $n \in X$ *(the* inductive step*)*

We then have that $X = \mathbb{N}$.

Once again, here's the intuitive argument for why induction is valid. By the first assumption, we know that $0 \in X$. Since $0 \in X$, the second assumption tells us that $1 \in X$. Since $1 \in X$, the second assumption again tells us that $2 \in X$. By repeatedly applying the second assumption in this manner, each element of $\mathbb{N}$ is eventually determined to be in X. Notice that a similar argument works if we start with a different base case, i.e. if we start by proving that $3 \in X$ and then prove the inductive step, then it follows that $n \in X$ for all $n \in \mathbb{N}$ with $n \geq 3$.

We now give many examples of proofs by induction.

Proposition 1.2. *For any $n \in \mathbb{N}^+$, we have*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Proof. We give a proof using induction.

- *Base Case:* For $n = 1$, the statement is true because $\frac{1 \cdot 2}{2} = 1$.
- *Inductive Step:* Assume that the statement is true for some fixed $n \in \mathbb{N}^+$, i.e. suppose that n is a number for which we know that
$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

We then have

$$\begin{aligned} 1+2+\cdots+n+(n+1) &= \frac{n(n+1)}{2}+(n+1) && \text{(by the inductive hypothesis)} \\ &= \frac{n^2+n+2n+2}{2} \\ &= \frac{n^2+3n+2}{2} \\ &= \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)((n+1)+1)}{2}. \end{aligned}$$

Thus, the statement is true for $n+1$.

By induction, we conclude that

$$1+2+\cdots+n = \frac{n(n+1)}{2}$$

is true for all $n \in \mathbb{N}^+$. □

Theorem 1.3. *For any $n \in \mathbb{N}^+$, we have*

$$\sum_{k=1}^{n}(2k-1) = n^2$$

i.e.

$$1+3+5+7+\cdots+(2n-1) = n^2$$

Proof. We give a proof by induction.

- *Base Case:* Suppose that $n = 1$. We have

  $$\sum_{k=1}^{1}(2k-1) = 2\cdot 1 - 1 = 1$$

  so the left hand-side is 1. The right-hand side is $1^2 = 1$. Thus, the statement is true when $n = 1$.

- *Inductive Step:* Assume that the statement is true for some fixed $n \in \mathbb{N}^+$, i.e. suppose that n is a number for which we know that

  $$\sum_{k=1}^{n}(2k-1) = n^2.$$

  Notice that $2(n+1)-1 = 2n+2-1 = 2n+1$, hence

  $$\begin{aligned} \sum_{k=1}^{n+1}(2k-1) &= [\sum_{k=1}^{n}(2k-1)] + [2(n+1)-1] \\ &= [\sum_{k=1}^{n}(2k-1)] + (2n+1) \\ &= n^2 + (2n+1) && \text{(by induction)} \\ &= (n+1)^2 \end{aligned}$$

  Thus, the statement is true for $n+1$.

By induction, we conclude that

$$\sum_{k=1}^{n}(2k-1) = n^2$$

for all $n \in \mathbb{N}^+$. □

We now formally define the concept of divisibility, which generalizes our definition of even beyond the number 2.

Definition 1.4. *Let $a, b \in \mathbb{Z}$. We say that a* divides *b, and write $a \mid b$, if there exists $m \in \mathbb{Z}$ with $b = am$.*

Proposition 1.5. *For all $n \in \mathbb{N}$, we have $3 \mid (4^n - 1)$.*

Proof. We give a proof by induction.

- *Base Case:* Suppose that $n = 0$. We have $4^0 - 1 = 1 - 1 = 0$, hence $3 \mid (4^0 - 1)$ because $3 \cdot 0 = 0$. Thus, the statement is true when $n = 0$.
- *Inductive Step:* Assume that the statement is true for some fixed $n \in \mathbb{N}^+$, i.e. suppose that n is a number for which we know that $3 \mid (4^n - 1)$. Fix $k \in \mathbb{Z}$ with $3k = 4^n - 1$. We then have

$$\begin{aligned} 4^{n+1} - 1 &= 4 \cdot 4^n - 1 \\ &= 4 \cdot (3k+1) - 1 \\ &= 12k - 3 \\ &= 3 \cdot (4k - 1) \end{aligned}$$

  Since $4k - 1 \in \mathbb{Z}$, we conclude that $3 \mid (4^{n+1} - 1)$. Thus, the statement is true for $n + 1$.

By induction, we conclude that $3 \mid (4^n - 1)$ for all $n \in \mathbb{N}$. □

Proposition 1.6. *We have $2n + 1 < n^2$ for all $n \in \mathbb{N}$ with $n \geq 3$.*

Proof. We give a proof by induction.

- *Base Case:* Suppose that $n = 3$. We have $2 \cdot 3 + 1 = 7$ and $3^2 = 9$, so $2 \cdot 3 + 1 < 3^2$. Thus, the statement is true when $n = 3$.
- *Inductive Step:* Assume that the statement is true for some fixed $n \in \mathbb{N}$ with $n \geq 3$, i.e. suppose that $n \geq 3$ is a number for which we know that $2n + 1 < n^2$. Since $2n + 1 \geq 2 \cdot 3 + 1 = 7 > 2$, we then have

$$\begin{aligned} 2(n+1) + 1 &= 2n + 3 \\ &= (2n+1) + 2 \\ &= n^2 + 2 \\ &< n^2 + 2n + 1 \\ &= (n+1)^2 \end{aligned}$$

  Thus, the statement is true for $n + 1$.

By induction, we conclude that $2n + 1 < n^2$ for all $n \in \mathbb{N}$ with $n \geq 3$. □

Proposition 1.7. *We have $n^2 < 2^n$ for all $n \geq 5$.*

Proof. We give a proof by induction.

- *Base Case:* Suppose that $n = 5$. We have $5^2 = 25$ and $2^5 = 32$, so $5^2 < 2^5$. Thus, the statement is true when $n = 5$.
- *Inductive Step:* Assume that the statement is true for some fixed $n \in \mathbb{N}$ with $n \geq 5$, i.e. suppose that $n \geq 5$ is a number for which we know that $n^2 < 2^n$. Since $n^2 = n \cdot n \geq 3n = 2n + n > 2n + 1$, we have then have

$$\begin{aligned}(n+1)^2 &= n^2 + 2n + 1 \\ &< n^2 + n^2 \\ &= 2n^2 \\ &< 2 \cdot 2^n \\ &= 2^{n+1}\end{aligned}$$

  Thus, the statement is true for $n + 1$.

By induction, we conclude that $n^2 < 2^n$ for all $n \geq 5$. □

Theorem 1.8. *For all $x \in \mathbb{R}$ with $x \geq -1$ and all $n \in \mathbb{N}^+$, we hve $(1 + x)^n \geq 1 + nx$.*

Proof. On the face of it, this looks a little different because it we are also quantifying over infinitely many real numbers x. Since x is coming from $\mathbb{R}$, we can't induct on x. However, we *can* take an arbitrary $x \in \mathbb{R}$ with $x \geq -1$, and then induct on n for this particular x. We now carry out that argument.

Let $x \in \mathbb{R}$ with $x \geq -1$. For this x, we show that $(1 + x)^n \geq 1 + nx$ for all $n \in \mathbb{N}^+$ by induction.

- *Base Case:* Suppose that $n = 1$. We then have that $(1 + x)^1 = 1 + x = 1 + 1x$, so certainly $(1 + x)^1 \geq 1 + 1x$.
- *Inductive Step:* Assume that the statement is true for some fixed $n \in \mathbb{N}^+$, i.e. suppose that n is a number for which we know that $(1 + x)^n \geq 1 + nx$. Since $x \geq -1$, we have $1 + x \geq 0$, so we can multiply both sides of this inequality by $(1 + x)$ to conclude that

$$(1 + x)^n \cdot (1 + x) \geq (1 + nx) \cdot (1 + x)$$

  We then have

$$\begin{aligned}(1+x)^{n+1} &= (1+x)^n \cdot (1+x) \\ &\geq (1+nx) \cdot (1+x) && \text{(from above)} \\ &= 1 + nx + x + nx^2 \\ &= 1 + (n+1)x + nx^2 \\ &\geq 1 + (n+1)x. && \text{(since } nx^2 \geq 0\text{)}\end{aligned}$$

  Hence, we have shown that $(1 + x)^{n+1} \geq 1 + (n + 1)x$, i.e. that the statement is true for $n + 1$.

By induction, we conclude that $(1 + x)^n \geq 1 + nx$ for all $n \in \mathbb{N}^+$. Since $x \in \mathbb{R}$ with $x \geq -1$ was arbitrary, the statement follows. □

Proposition 1.9. *Suppose that $a, b \in \mathbb{Z}$. If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.*

Proof. Suppose that $a \mid b$ and $b \neq 0$. Fix $d \in \mathbb{Z}$ with $ad = b$. Since $b \neq 0$, we have $d \neq 0$. Thus, $|d| \geq 1$, and so

$$|b| = |ad| = |a| \cdot |d| \geq |a| \cdot 1 = |a|$$

The result follows. □

Theorem 1.10. *Let $a, b \in \mathbb{N}$ with $b \neq 0$. There exist unique $q, r \in \mathbb{N}$ such that $a = qb + r$ and $0 \leq r < b$. Uniqueness here means that if $a = q_1 b + r_1$ with $0 \leq r_1 < b$ and $a = q_2 b + r_2$ with $0 \leq r_2 < b$, then $q_1 = q_2$ and $r_1 = r_2$.*

Proof. We first prove existence. Since we want to prove something for all $a, b \in \mathbb{N}$, it might at first seem unclear how to apply induction to both a and b. The answer in this case is not to induct on both, but to fix b and induct on a. In other words, let $b \in \mathbb{N}$ with $b > 0$ be arbitrary, and for this fixed b, we prove the existence of q, r for all $a \in \mathbb{N}$ by induction on a. That is, for this fixed b, we define

$$X = \{a \in \mathbb{N} : \text{ There exist } q, r \in \mathbb{N} \text{ with } a = qb + r\}$$

and show that $X = \mathbb{N}$ by induction.

- *Base Case:* Suppose that $a = 0$. We then have $a = 0 \cdot b + 0$ and since $0 < b$, we may take $q = 0$ and $r = 0$.
- *Inductive Step:* Assume that the statement is true for some fixed $a \in \mathbb{N}$. Fix $q, r \in \mathbb{Z}$ with $0 \leq r < b$ such that $a = qb + r$. We then have $a + 1 = qb + (r + 1)$. Since $r, b \in \mathbb{N}$ with $r < b$, we know that $r + 1 \leq b$. If $r + 1 < b$, then we are done. Otherwise, we have $r + 1 = b$, hence

$$\begin{aligned} a + 1 &= qb + (r + 1) \\ &= qb + b \\ &= (q + 1)b \\ &= (q + 1)b + 0 \end{aligned}$$

  and so we may take $q + 1$ and 0. Thus, the statement is true for $a + 1$.

Therefore, the existence part of the theorem follows by induction.

We now prove uniqueness. Let $a, b \in \mathbb{N}$ with $b \neq 0$. Suppose that $q_1, q_2, r_1, r_2 \in \mathbb{N}$ are such that

$$q_1 b + r_1 = a = q_2 b + r_2$$

and both $0 \leq r_1 < b$ and $0 \leq r_2 < b$. We then have

$$b(q_2 - q_1) = r_1 - r_2$$

hence $b \mid (r_2 - r_1)$. Now $-b < -r_1 \leq 0$, so adding this to $0 \leq r_2 < b$, we conclude that

$$-b < r_2 - r_1 < b$$

and therefore

$$|r_2 - r_1| < b$$

Now if $r_2 - r_1 \neq 0$, then since $b \mid (r_2 - r_1)$, we would conclude from Proposition 1.9 that $|b| \leq |r_2 - r_1|$, a contradiction. It follows that $r_2 - r_1 = 0$, and hence $r_1 = r_2$. Since

$$q_1 b + r_1 = q_2 b + r_2$$

and $r_1 = r_2$, we conclude that $q_1 b = q_2 b$. Now $b \neq 0$, so it follows that $q_1 = q_2$. □

Proposition 1.11. *Let $a, b \in \mathbb{N}$ with $b \neq 0$. Write $a = qb + r$ for the unique choice of $q, r \in \mathbb{N}$ with $0 \leq r < b$. We then have that $b \mid a$ if and only if $r = 0$.*

Proof. If $r = 0$, then $a = qb + r = bq$, so $b \mid a$. Suppose conversely that $b \mid a$ and fix $m \in \mathbb{Z}$ with $a = bm$. Notice that since $a \geq 0$ and $b \geq 0$, we must have that $m \geq 0$. We then have that both $a = mb + 0$ and $a = qb + r$, so by the uniqueness part of the above theorem, we must have $r = 0$. □