Strong Induction

Joseph R. Mileti

February 13, 2015

1 Strong Induction

Remember our original model for induction:

- 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.
- Prove that if the statement is true for 3, then the statement is true for 4.
- ....

In the previous section, we argued why this model was sound and gave many examples. However, upon closer inspection, it appears that we can assume more. In the second line, when proving that the statement is true for 1 we are allowed to assume that the statement is true for 0. Now in the third line, when proving that the statement is true for 2, we only assume that it is true for 1. If we are knocking down the natural numbers in order, then we've already proved that it's true for 0, so why can't we assume that as well? The answer is that we can indeed assume it, and in general when working to prove that the statement is true for a natural number n, we can assume that we know it is true for all smaller values. In other words, we do 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 0 and 1, then the statement is true for 2.
- Prove that if the statement is true for 0, 1, and 2, then the statement is true for 3.
- Prove that if the statement is true for 0, 1, 2, and 3, then the statement is true for 4.
- ....

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 both 0 and 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.

As usual, 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 each of $0, 1, 2, \ldots, n$, then the statement is true for $n + 1$.

Alternatively, we can state this as follows:

- Prove that the statement is true for 0.
- Prove that if the statement is true for each of $0, 1, 2, \ldots, n - 1$, then the statement is true for n (for $n \geq 1$).

An argument using these method is called a proof by *strong induction*. As we will see in the examples below, sometimes we need to modify this clean structure to include several base cases to get the argument going. Rather than going through a theoretical discussion of how and why one would do this, it's easier to illustrate the technique by example.

Proposition 1.1. *Define a sequence a_n recursively by letting $a_0 = 0$, $a_1 = 1$, and*

$$a_n = 3a_{n-1} - 2a_{n-2}$$

for $n \geq 2$. Show that $a_n = 2^n - 1$ for all $n \in \mathbb{N}$.

Proof. We prove that $a_n = 2^n - 1$ for all $n \in \mathbb{N}$ by strong induction.

- *Base Case:* We handle two bases where $n = 0$ and $n = 1$ because our inductive step will use the result for two steps back. When $n = 0$, we have $a_0 = 0$ and $2^0 - 1 = 1 - 1 = 0$, so $a_0 = 2^0 - 1$. When $n = 1$, we have $a_1 = 1$ and $2^1 - 1 = 2 - 1 = 1$, so $a_1 = 2^1 - 1$.
- *Inductive Step:* Let $n \geq 2$ and assume that the statement is true for $0, 1, 2, \ldots, n - 1$, i.e. assume that $a_m = 2^m - 1$ for all $m \in \{0, 1, 2, \ldots, n - 1\}$. We prove that the statement is true for n. Notice that since $n \geq 2$, we have $0 \leq n - 1 < n$ and $0 \leq n - 2 < n$, so we know that $a_{n-1} = 2^{n-1} - 1$ and $a_{n-2} = 2^{n-2} - 1$. Now

$$\begin{aligned}
a_n &= 3a_{n-1} - 2a_{n-1} && \text{(by definition since } n \geq 2\text{)} \\
&= 3 \cdot (2^{n-1} - 1) - 2 \cdot (2^{n-2} - 1) && \text{(by the inductive hypothesis)} \\
&= 3 \cdot 2^{n-1} - 3 - 2 \cdot 2^{n-2} + 2 \\
&= 3 \cdot 2^{n-1} - 2^{n-1} - 1 \\
&= (3 - 1) \cdot 2^{n-1} - 1 \\
&= 2 \cdot 2^{n-1} - 1 \\
&= 2^n - 1
\end{aligned}$$

  Thus, $a_n = 2^n - 1$ and so the statement is true for n.

Using strong induction, we conclude that $a_n = 2^n - 1$ for all $n \in \mathbb{N}$. □

Proposition 1.2. *If $n \in \mathbb{N}$ and $n \geq 12$, then there exist $k, \ell \in \mathbb{N}$ with $n = 4k + 5\ell$.*

Proof. We give a proof by strong induction.

- *Base Case:* We first prove that the statement is true for $n \in \{12, 13, 14, 15\}$ (we will see why we need so many base cases below). We have
  - $12 = 4 \cdot 3 + 5 \cdot 0$

- $13 = 4 \cdot 2 + 5 \cdot 1$
- $14 = 4 \cdot 1 + 5 \cdot 2$
- $15 = 4 \cdot 0 + 5 \cdot 3$

Thus, the statement is true for $n \in \{12, 13, 14, 15\}$.

- *Inductive Step:* Let $n \geq 16$ and assume that the statement is true for $12, 13, 14, \ldots, n-1$. We prove that the statement is true for n. Since $n \geq 16$, we have $12 \leq n-4 < n$. Since $12 \leq n-4 < 4$, we know that there exists $k, \ell \in \mathbb{N}$ with

$$n - 4 = 4k + 5\ell.$$

Adding 4 to both sides, we conclude that

$$n = 4k + 5\ell + 4 = 4(k+1) + 5\ell$$

Since $k+1, \ell \in \mathbb{N}$, we conclude that the statement is true for n.

By (strong) induction, we conclude that for all $n \in \mathbb{N}$ with $n \geq 12$, there exist $k, \ell \in \mathbb{N}$ with $n = 4k + 5\ell$. □

Theorem 1.3. *Let $b \in \mathbb{N}$ with $b \geq 2$. For all $n \in \mathbb{N}^+$, there exists $a_0, a_1, a_2, \ldots, a_k \in \mathbb{N}$ with $0 \leq a_i < b$ for all i such that*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

Proof. Let $b \in \mathbb{N}$ with $b \geq 2$ be arbitrary. With this fixed b, we prove the result by strong induction on n.

- *Base Case:* Let $n = 1$. We may take $k = 1$ and $a_0 = 1 < b$.
- *Inductive Step:* Let $n \geq 2$ and assume that the statement is true for $1, 2, \ldots, n-1$. Fix $q, r \in \mathbb{N}$ with $n = qb + r$ and $0 \leq r < b$. Notice that $q < n$ because $q \geq n$ would imply that

$$n = qb + r \geq qb \geq nb \geq 2n > n$$

a contradiction. Therefore, since $0 \leq q < n$, we may use strong induction to conclude that we can fix $a_0, a_1, a_2, \ldots, a_k \in \mathbb{N}$ with $0 \leq a_i < b$ for all i such that

$$q = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0.$$

We then have

$$\begin{aligned} n &= qb + r \\ &= (a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0) b + r \\ &= a_k b^{k+1} + a_{k-1} b^k + \cdots + a_1 b^2 + a_0 b + r \end{aligned}$$

Since $0 \leq r < b$, we have shown that the statement is true for n.

The result follows by induction. □

We now turn our attention back to divisibility. We begin with a fundamental result.

Proposition 1.4. *Let $a, b, c \in \mathbb{Z}$.*

1. *If $a \mid b$, then $a \mid bk$ for all $k \in \mathbb{Z}$.*
2. *If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*

3. If $a \mid b$ and $a \mid c$, then $a \mid (bk + c\ell)$ for all $k, \ell \in \mathbb{Z}$.

Proof.

1. Suppose that $a \mid b$. Let $k \in \mathbb{Z}$ be arbitrary. Since $a \mid b$, we may fix $m \in \mathbb{Z}$ with $b = am$. We then have
$$bk = (am)k = a(mk)$$
Since $mk \in \mathbb{Z}$, it follows that $a \mid bk$. Since $k \in \mathbb{Z}$ was arbitrary, the result follows.

2. Suppose that $a \mid b$ and $a \mid c$. Since $a \mid b$, we may fix $m \in \mathbb{Z}$ with $b = am$. Since $a \mid c$, we may fix $n \in \mathbb{Z}$ with $c = an$. We then have
$$b + c = am + an = a(m + n)$$
Since $m + n \in \mathbb{Z}$, it follows that $a \mid b + c$.

3. This follows by combining 1 and 2 as follows. Suppose that $a \mid b$ and $a \mid c$. Let $m, n \in \mathbb{Z}$ be arbitrary. Since $a \mid b$, we conclude from part 1 that $a \mid bm$. Since $a \mid c$, we conclude from part 1 again that $a \mid cn$. Using part 2, it follows that $a \mid (bm + cn)$. Since $m, n \in \mathbb{Z}$ were arbitrary, the result follows. Alternatively, you should try to prove this directly without using the first two parts.

□

Definition 1.5. *Suppose that $a, b \in \mathbb{Z}$. We say that $d \in \mathbb{Z}$ is a* common divisor *of a and b if both $d \mid a$ and $d \mid b$.*

The common divisors of 120 and 84 are $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$ (we will see a careful argument below). The common divisors of 10 and 0 are $\{\pm 1, \pm 2, \pm 5, \pm 10\}$. Every element of $\mathbb{Z}$ is a common divisor of 0 and 0. The following little proposition is fundamental to this entire section.

Proposition 1.6. *Suppose that $a, b, q, r \in \mathbb{Z}$ and $a = qb + r$ (we need not have $0 \leq r < |b|$). For any $d \in \mathbb{Z}$, we have that d is a common divisor of a and b if and only if d is a common divisor of b and r, i.e.*
$$\{d \in \mathbb{Z} : d \text{ is a common divisor of } a \text{ and } b\} = \{d \in \mathbb{Z} : d \text{ is a common divisor of } b \text{ and } r\}.$$

Proof. Suppose first that d is a common divisor of b and r. Since $d \mid b$, $d \mid r$, and $a = qb + r = bq + r1$, we may use Proposition 1.4 to conclude that $d \mid a$.

Conversely, suppose that d is a common divisor of a and b. Since $d \mid a$, $d \mid b$, and $r = a - qb = a1 + b(-q)$, we may use Proposition 1.4 to conclude that $d \mid r$. □

For example, suppose that we are trying to find the set of common divisors of 120 and 84 (we wrote them above, but now want to justify it). We repeatedly do division to reduce the problem as follows:
$$\begin{aligned} 120 &= 1 \cdot 84 + 36 \\ 84 &= 2 \cdot 36 + 12 \\ 36 &= 3 \cdot 12 + 0 \end{aligned}$$
The first line tells us that the set of common divisors of 120 and 84 equals the set of common divisors of 84 and 36. The next line tells us that the set of common divisors of 84 and 36 equals the set of common divisors of 36 and 12. The last line tells us that the set of common divisors of 36 and 12 equals the set of common divisors of 12 and 0. Now the set of common divisors of 12 and 0 is simply the set of divisors of 12 (because every number divides 0). Putting it all together, we conclude that the set of common divisors of 120 and 84 equals the set of divisors of 12.

Definition 1.7. *Let $a, b \in \mathbb{Z}$. We say that an element $d \in \mathbb{Z}$ is a* greatest common divisor *of a and b if:*

- $d \geq 0$
- *d is a common divisor of a and b.*
- *Whenever $c \in \mathbb{Z}$ is a common divisor of a and b, we have $c \mid d$.*

Notice that we are *not* defining the greatest common divisor of a and b to be the largest divisor of a and b. The primary reason we do not is because this description fails to capture the most fundamental property (namely that of being divisible by all other divisors, not just larger than them). Furthermore, if we were to take that definition, then 0 and 0 would fail to have a greatest common divisor because every integer is a common divisor of 0 and 0. With this definition however, it is a straightforward matter to check that 0 satisfies the above three conditions.

Since we require more of a greatest common divisor than just picking the largest, we first need to check that they do indeed exist. The proof is an inductive formulation of the above method of calculation.

Theorem 1.8. *Every pair of integers $a, b \in \mathbb{Z}$ has a unique greatest common divisor.*

We first sketch the idea of the proof in the case where $a, b \in \mathbb{N}$. If $b = 0$, we are done because it is simple to verify that a is a greatest common divisor of a and 0. Suppose then that $b \neq 0$. Fix $q, r \in \mathbb{N}$ with $a = qb + r$ and $0 \leq r < b$. Now the idea is to assert inductively the existence of a greatest common divisor of b and r because this pair is "smaller" than the pair a and b. The only issue is how to make this intuitive idea of "smaller" precise. There are several ways to do this, but perhaps the most straightforward is to only induct on b. Thus, our base case handles all pairs of form $(a, 0)$. Next, we handle all pairs of the form $(a, 1)$ and in doing this we can use the fact the we know the result for all pairs of the form $(a', 0)$. Notice that we can we even change the value of the first coordinate here which is why we used a'. Then, we handle all pairs of the form $(a, 2)$ and in doing this we can use the fact that we know the result for all pairs of the form $(a', 0)$ and $(a', 1)$. We now begin the formal argument.

Proof. We begin by proving existence only in the special case where $a, b \in \mathbb{N}$. We use (strong) induction on b to prove the result. That is, we let

$$X = \{b \in \mathbb{N} : \text{For all } a \in \mathbb{N}, \text{ there exists a greatest common divisor of } a \text{ and } b\}$$

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

- *Base Case:* Suppose that $b = 0$. Let $a \in \mathbb{N}$ be arbitrary. We then have that the set of common divisors of a and b equals the set of divisors of a (because every integer divides 0), so a satisfies the requirement of a greatest common divisor of a and 0. Since $a \in \mathbb{N}$ was arbitrary, we showed that there exists a greatest common divisor of a and 0 for every $a \in \mathbb{N}$, hence $0 \in X$.
- *Inductive Step:* Suppose then that $b \in \mathbb{N}^+$ and we know the result for all smaller natural numbers. In other words, we are assuming that $c \in X$ whenever $0 \leq c < b$. We prove that $b \in X$. Let $a \in \mathbb{N}$ be arbitrary. From above, we may fix $q, r \in \mathbb{Z}$ with $a = qb + r$ and $0 \leq r < b$. Since $0 \leq r < b$, we know by strong induction that $r \in X$, hence b and r have a greatest common divisor d. By Proposition 1.6, the set of common divisors of a and b equals the set of common divisors of b and r. It follows that d is a greatest common divisor of a and b. Since $a \in \mathbb{N}$ was arbitrary, we showed that there exists a greatest common divisor of a and b for every $a \in \mathbb{N}$, hence $b \in X$.

Therefore, we have shown that $X = \mathbb{N}$, which implies that whenever $a, b \in \mathbb{N}$, there exists a greatest common divisor of a and b.

To turn the argument into a proof for all $a, b \in \mathbb{Z}$, we simply note the set of divisors of an element $m \in \mathbb{Z}$ equals the set of divisors of $-m$. So, for example, if $a < 0$ but $b \geq 0$ we can simply take a greatest common divisor of $-a$ and b (which exists since $-a, b \in \mathbb{N}$) and note that it will also be a greatest common divisor of a and b. A similar argument works if $a \geq 0$ and $b < 0$, or if both $a < 0$ and $b < 0$.

For uniqueness, suppose that c and d are both greatest common divisors of a and b. Since d is a greatest common divisor and c is a common divisor, we know by the last condition that $c \mid d$. Similarly, since c is a greatest common divisor and d is a common divisor, we know by the last condition that $d \mid c$. Therefore, either $c = d$ or $c = -d$. Using the first requirement that a greatest common divisor must be nonnegative, we must have $c = d$. □

Definition 1.9. *Let $a, b \in \mathbb{Z}$. We let $\gcd(a, b)$ be the unique greatest common divisor of a and b.*

For example we have $\gcd(120, 84) = 12$ and $\gcd(0, 0) = 0$. The following corollary is immediate from Proposition 1.6.

Corollary 1.10. *Suppose that $a, b, q, r \in \mathbb{Z}$ and $a = qb + r$. We have $\gcd(a, b) = \gcd(b, r)$.*

The method of using repeated division and this corollary to reduce the problem of calculating greatest common divisors is known as the *Euclidean Algorithm*. We saw it in action of above with 120 and 84. Here is another example where we are trying to compute $\gcd(525, 182)$. We have

$$\begin{aligned} 525 &= 2 \cdot 182 + 161 \\ 182 &= 1 \cdot 161 + 21 \\ 161 &= 7 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0 \end{aligned}$$

Therefore, $\gcd(525, 182) = \gcd(7, 0) = 7$.

Theorem 1.11. *For all $a, b \in \mathbb{Z}$, there exist $k, \ell \in \mathbb{Z}$ with $\gcd(a, b) = ka + \ell b$.*

Proof. We begin by proving existence in the special case where $a, b \in \mathbb{N}$. We use induction on b to prove the result. That is, we let

$$X = \{b \in \mathbb{N} : \text{For all } a \in \mathbb{N}, \text{ there exist } k, \ell \in \mathbb{Z} \text{ with } \gcd(a, b) = ka + \ell b\}$$

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

- *Base Case:* Suppose that $b = 0$. Let $a \in \mathbb{N}$ be arbitrary. We then have that

  $$\gcd(a, b) = \gcd(a, 0) = a$$

  Since $a = 1 \cdot a + 0 \cdot b$, so we may let $k = 1$ and $\ell = 0$. Since $a \in \mathbb{N}$ was arbitrary, we conclude that $0 \in X$.

- *Inductive Step:* Suppose then that $b \in \mathbb{N}^+$ and we know the result for all smaller nonnegative values. In other words, we are assuming that $c \in X$ whenever $0 \leq c < b$. We prove that $b \in X$. Let $a \in \mathbb{N}$ be arbitrary. From above, we may fix $q, r \in \mathbb{Z}$ with $a = qb + r$ and $0 \leq r < b$. We also know from above that $\gcd(a, b) = \gcd(b, r)$. Since $0 \leq r < b$, we know by strong induction that $r \in X$, hence there exist $k, \ell \in \mathbb{Z}$ with

  $$\gcd(b, r) = kb + \ell r$$

  Now $r = a - qb$, so

  $$\begin{aligned} \gcd(a, b) &= \gcd(b, r) \\ &= kb + \ell r \\ &= kb + \ell(a - qb) \\ &= kb + \ell a - qb\ell \\ &= \ell a + (k - q\ell)b \end{aligned}$$

  Since $a \in \mathbb{N}$ was arbitrary, we conclude that $b \in X$.

Therefore, we have shown that $X = \mathbb{N}$, which implies that whenever $a, b \in \mathbb{N}$, there exists $k, \ell \in \mathbb{Z}$ with $\gcd(a, b) = ka + \ell b$. □

Given $a, b \in \mathbb{Z}$, we can explicitly calculate $k, \ell \in \mathbb{Z}$ by "winding up" the work created from the Euclidean Algorithm. For example, we saw above that $\gcd(525, 182) = 7$ by calculating

$$\begin{aligned} 525 &= 2 \cdot 182 + 161 \\ 182 &= 1 \cdot 161 + 21 \\ 161 &= 7 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0 \end{aligned}$$

We now use these steps in reverse to calculate:

$$\begin{aligned} 7 &= 1 \cdot 7 + 0 \cdot 0 \\ &= 1 \cdot 7 + 0 \cdot (14 - 2 \cdot 7) \\ &= 0 \cdot 14 + 1 \cdot 7 \\ &= 0 \cdot 14 + 1 \cdot (21 - 1 \cdot 14) \\ &= 1 \cdot 21 + (-1) \cdot 14 \\ &= 1 \cdot 21 + (-1) \cdot (161 - 7 \cdot 21) \\ &= (-1) \cdot 161 + 8 \cdot 21 \\ &= (-1) \cdot 161 + 8 \cdot (182 - 1 \cdot 161) \\ &= 8 \cdot 182 + (-9) \cdot 161 \\ &= 8 \cdot 182 + (-9) \cdot (525 - 2 \cdot 182) \\ &= (-9) \cdot 525 + 26 \cdot 182 \end{aligned}$$

This wraps everything up perfectly, but it is easier to simply start at the fifth line.

We end this section with a useful result.

Definition 1.12. *Two elements $a, b \in \mathbb{Z}$ are* relatively prime *if* $\gcd(a, b) = 1$.

Proposition 1.13. *Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. Since $a \mid bc$, we may fix $m \in \mathbb{Z}$ with $bc = am$. Since $\gcd(a, b) = 1$, we may fix $k, \ell \in \mathbb{Z}$ with $ak + b\ell = 1$. Multiplying this last equation through by c we conclude that $akc + b\ell c = c$, so

$$\begin{aligned} c &= akc + \ell(bc) \\ &= akc + na\ell \\ &= a(kc + n\ell) \end{aligned}$$

It follows that $a \mid c$. □