Strong Induction[1]

- **Making Life Easier.**

  In the inductive case mentioned last time, we needed to show $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n+1)$ is true. It actually suffices to prove an easier statement.

  - **Base Case:** $P(1)$ is true; and
  - **Inductive Case:** For all $n \in \mathbb{N}$, if $P(n), P(n-1), \ldots, P(1)$ is true (*the induction hypothesis*), then $P(n+1)$ is true,

  then, $P(n)$ is true for all $n \in \mathbb{N}$.

  Since we assume more things to prove the same thing, the above is often easier to establish. This way of proving is often called ***strong induction.***

  > **Remark:** *Personally, I am not a big fan of these different names. In my day-to-day life, I call both of these methods just plain induction. But if it helps you, please make the distinction. I will try to do so in class.*

- **Prime Factorization.**

  > **Theorem 1.** Every natural number ≥ 2 can be written as a product of primes and 1.

  Proof. Let $P(n)$ be the predicate which takes the value true if the number n can be written as a product of primes. We need to prove $\forall n \in \mathbb{N}, n \geq 2 : P(n)$. We proceed by induction.

  Base Case: Note that the base case is $P(2)$ (and not $P(1)$ since that is not asserted to be true). Indeed $2 = 2 \times 1$ can be written as a product of primes and 1; therefore $P(2)$ is true.

  Inductive Case: Fix a natural number $k \geq 2$. Assume $P(k), P(k-1), \ldots, P(2)$ are all true. We need to establish $P(k+1)$. That is, we need to prove $(k+1)$ can be written as a product of primes ad 1.

  Case 1: $(k+1)$ is a prime. In this case, there is nothing to show; $(k+1) = (k+1) \times 1$ is a product of the single prime $(k+1)$ and 1.

  Case 2: $(k+1)$ is *not* a prime. This implies, there exists two natural numbers a and b such that (i) $2 \leq a \leq k$ and $2 \leq b \leq k$, and (ii) $(k+1) = a \cdot b$.

  By the inductive hypothesis, $P(a)$ and $P(b)$ are both true (note, the "weak" induction wouldn't have told us this). Therefore, a can be written as product of primes and 1, and b can be written as a product of primes and 1, and therefore, $a \cdot b$ can be written as a product of primes and 1. That is, $(k+1)$ can be written as a product of primes and 1. We have therefore established $P(k+1)$ is true.

  By (strong) induction, therefore, $\forall n \geq 2, n \in \mathbb{N} : P(n)$ is true. ☐

[1] *Lecture notes by Deeparnab Chakrabarty. Last modified : 28th Aug, 2021*
These have not gone through scrutiny and may contain errors. If you find any, or have any other comments, please email me at deeparnab@dartmouth.edu. Highly appreciated!

Remark: *Does the theorem above prove that every natural number ≥ 2 can be* **uniquely** *written as a product of primes? It doesn't. Convince yourself of this fact. Hint: $(k+1)$ can indeed be written as $a \cdot b$ and $c \cdot d$ for different $(a, b), (c, d)$ tuples. For example, $36 = 4 \cdot 9 = 6 \cdot 6$. Can you massage the above proof to prove uniqueness?*

- **The Change Problem.** In the country of Borduria, they have three types of coins: a cent, a szlapot, and a dinar. A szlapot is worth 3 cents and a dinar is worth 7 cents. You have an unending supply of szlapots and dinars; show that any amount ≥ 12 cents can be made with only szlapots and dinars.

  You may have heard of similar such puzzles. In Math terms, it is stating the following theorem.

Theorem 2. Prove that any natural number $n \geq 12$ can be expressed as $3x + 7y$ for *non-negative integers* x and y.

Proof. Let $P(n)$ be the predicate taking the value `true` if there exist non-negative integers (x, y) such that $n = 3x + 7y$. We need to prove $\forall n \geq 12, n \in \mathbb{N} : P(n)$.

Base Case: Again, the base case here is $P(12)$, and indeed, $12 = 3 \cdot 4 + 7 \cdot 0$, and thus $P(12)$ is true. With hindsight, we know that just checking this will not suffice. So we go ahead and check $P(13)$ and $P(14)$ as well. Indeed, $13 = 3 \times 2 + 7 \times 1$, and $14 = 3 \times 0 + 7 \times 2$.

Inductive Case: Since we have established $P(12), P(13), P(14)$ we need to establish $P(k)$ for $k > 14$. Fix a $k \geq 14$. The Induction Hypothesis is that $P(12), P(13), \ldots, P(k)$ are true. We now need to prove $P(k+1)$. That is, we need to find a way to write $(k+1)$ as $3x + 7y$ for some non-negative integers (x, y).

To see this, consider the number $m := (k+1) - 3$. Since $k \geq 14$, we see $m \geq 12$. Also, $m < (k+1)$, and therefore, $P(m)$ is true. That is, there exists non-negative integers (x', y') such that $m = 3x' + 7y'$. But $(k+1) = m + 3$, and therefore, $(k+1) = 3(x'+1) + 7y'$. Since $x' \geq 0$, $x' + 1 \geq 0$ as well. Therefore, $(k+1)$ is expressed as $3x + 7y$ with non-negative integers $x = x' + 1$ and $y = y'$. Thus, $P(k+1)$ is proved, and by induction, $P(n)$ is proved for all $n \geq 12$. □

Remark: *In fact, the above proof also shows that any number $n \geq 12$ can be written as $3x + 7y$ where x and y are non-negative integers* and $y \leq 2$. *Do you see it? Make sure you see it.*

Note that the above proof also implies a *recursive* algorithm to find the changes for any given number N.

```
procedure FindChange(N): ▷ N ≥ 12. Returns (x, y) such that N = 3x + 7y.
    ▷ First take care of base cases
    if N = 12 then: return (4, 0).
    if N = 13 then: return (2, 1).
    if N = 14 then: return (0, 2).
    ▷ If we haven't returned yet, then N ≥ 15. In which case, inductive case.
    (x', y') ← FindChange(N − 3)
    return (x' + 1, y').
```

Remark: *There is a generalization of this problem which is called the* **Frobenius problem**. *It asks, given n non-negative integers $a_1, a_2, \ldots, a_n$ such that $\gcd(a_1, a_2, \ldots, a_n) = 1$ (that is, there is no number > 1 which divides all of the a_i's), find the* largest *number which* cannot *be expressed as $a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots a_n \cdot x_n$ for non-negative integers $x_1, \ldots, x_n$. Note that the above theorem shows that when $a_1 = 3$ and $a_2 = 7$, the largest number is 11. So the answer to the Frobenius problem for $(3, 7)$ is 11. Can you show that for any $(a_1, \ldots, a_n)$, there is some* finite *number $F(a_1, \ldots, a_n)$ which is the answer to the above question?*

- **Strengthening the Induction Hypothesis**

To get an idea of this, first try and prove this statement by induction.

Theorem 3. For any natural number n, prove that $\left(1 + \frac{1}{n}\right)^n \geq 2$.

Could you do it?

I am going to use this as an opportunity to tell one quite non-intuitive facts about proofs by induction:

It is often easier to prove something stronger.

What do I mean? Well, consider the following theorem.

Theorem 4. Fix any $x \geq -1$. Then $\forall n \in \mathbb{N}$ we have $(1 + x)^n \geq 1 + nx$.

Obsereve that Theorem 4 *implies* Theorem 3; indeed, if we set $x = n$ we get the statement of Theorem 3. Therefore, it should be only *harder* to prove Theorem 4. Turns out, that is not the case.

Proof. Fix an arbitrary real $x \geq -1$. Let $P(n)$ be the predicate which is true if $(1 + x)^n \geq 1 + nx$. We need to show $\forall n \in \mathbb{N} : P(n)$ is true. We proceed by induction.

Base Case. Let us first establish $P(1)$ is true. That is, $(1 + x)^1 \geq 1 + 1 \cdot x$; indeed they are equal.

Inductive Case. Fix a natural number $k \geq 1$ and assume $P(k)$ is true. That is, we assume

$$(1 + x)^k \geq 1 + kx \tag{IH}$$

We need to show $P(k+1)$ is true. That is, we need to show

$$(1+x)^{k+1} \geq 1+(k+1)x \tag{Need to Show}$$

Indeed,

$$\begin{aligned}
(1+x)^{k+1} &= (1+x)^k \cdot (1+x) \\
&\geq (1+kx) \cdot (1+x) \; 1+x \geq 0 \text{ since } x \geq -1. \\
&= 1+kx+x+kx^2 \\
&\geq \quad 1+(k+1)x
\end{aligned}$$

Thus, $P(k+1)$ is true, and we have proved the theorem via induction. □