Recall proof by induction:

1. Show a base case: show that $P(n_0)$ is true.
2. Induction step: show $P(n) \Rightarrow P(n+1)$ for all $n \geqslant n_0$.

Then since $\Rightarrow$ is "transitive", we have proven $P(k)$ for all $k \geqslant n_0$.

For example, we proved

$$P(n): \qquad \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

by checking

$$P(1): \qquad \sum_{i=1}^{1} i = 1 = \frac{1(2)}{2}\checkmark,$$

and $P(n) \Rightarrow P(n+1)$:

$$\sum_{i=1}^{n+1} i = \left(\sum_{i=1}^{n} i\right) + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}\checkmark.$$

So for any $k \geqslant 1$, we have $P(1)$ is true and

$$P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow \cdots \Rightarrow P(k-1) \Rightarrow P(k),$$

so $P(k)$ is true too!

Proof by induction:

1. Show a base case: show that $P(n_0)$ is true.
2. Induction step: show $P(n) \Rightarrow P(n+1)$ for all $n \geqslant n_0$.
   "Fix $n \geqslant n_0$ and assume $P(n)$. $\leftarrow$ *Induction hypothesis*
   Then .... So $P(n+1)$ is true." $\leftarrow$ *Induction step*

A variant on induction: Strong Induction

1. Show a base case: show that $P(n_0)$ is true.
2. Induction step: show

$$\left(\bigwedge_{i=n_0}^{n} P(i)\right) \Rightarrow P(n+1)$$

   for all $n \geqslant n_0$.
   "Fix $n \geqslant n_0$ and assume $P(k)$ for all $n_0 \leqslant k \leqslant n$.
   $\nwarrow$ *(Strong) induction hypothesis*
   Then .... So $P(n+1)$ is true." $\leftarrow$ *Induction step*

Theorem. (The Fundamental Theorem of Arithmetic) Every integer $n \geqslant 2$ can be factored as

$$n = p_1 p_2 \cdots p_r$$

with $p_1, p_2, \ldots, p_r$ prime (not necessarily distinct).

Proof by strong induction (1^{st} draft). Let $P(n)$ be the thm statement.
Base case: 2 is prime, so the statement holds for $n = 2$. ✓
Goal: Assume $P(k)$ for all $2 \leqslant k \leqslant n$, and show $n+1$ has a factorization into primes.
Induction step: Fix $n \geqslant 2$ and assume that k has a prime factorization for all $2 \leqslant k \leqslant n$. Now consider $n+1$. Either $n+1$ is prime, or $n+1 = xy$ for some integers $2 \leqslant x, y \leqslant n$. By the induction hypothesis, there are primes $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ so that

$$x = p_1 p_2 \cdots p_r \quad \text{and} \quad y = q_1 q_2 \cdots q_s.$$

So

$$n + 1 = xy = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s. \checkmark$$

Conclusion. Since $P(2)$ holds, and $\left(\bigwedge_{k=n_0}^{n} P(i)\right) \Rightarrow P(n+1)$ for all $n \geqslant 2$, we have $P(\ell)$ for all $\ell \geqslant 2$.

Theorem. (The Fundamental Theorem of Arithmetic) Every integer $n \geqslant 2$ can be factored as

$$n = p_1 p_2 \cdots p_r$$

with $p_1, p_2, \ldots, p_r$ prime (not necessarily distinct).

Proof by strong induction (1^{st} draft).
Basically, we just showed

$$\begin{aligned}
&P(2)\\
P(2) &\Rightarrow P(3)\\
\big(P(2) \wedge P(3)\big) &\Rightarrow P(4)\\
\big(P(2) \wedge P(3) \wedge P(4)\big) &\Rightarrow P(5)\\
\big(P(2) \wedge P(3) \wedge P(4) \wedge P(5)\big) &\Rightarrow P(6)\\
&\vdots\\
\big(P(2) \wedge P(3) \wedge \cdots \wedge P(n)\big) &\Rightarrow P(n+1)
\end{aligned}$$

Theorem. (The Fundamental Theorem of Arithmetic) Every integer $n \geqslant 2$ can be factored as

$$n = p_1 p_2 \cdots p_r$$

with $p_1, p_2, \ldots, p_r$ prime (not necessarily distinct).

Proof by strong induction (Final draft). First, 2 is prime, so the statement holds for $n = 2$. Next, fix $n \geqslant 2$ and assume k has a prime factorization for all $2 \leqslant k \leqslant n$. Now, considering $n+1$, either $n+1$ is prime, or $n+1 = xy$ for some integers $2 \leqslant x, y \leqslant n$. By the induction hypothesis, there are primes $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ so that

$$x = p_1 p_2 \cdots p_r \quad \text{and} \quad y = q_1 q_2 \cdots q_s.$$

So

$$n+1 = xy = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s. \checkmark$$

Thus, by strong induction, the claim holds for all $n \geqslant 2$.

Claim: A chocolate bar consists of unit squares arranged in an $n \times m$ rectangular grid. There's a way to split the bar into individual unit squares by breaking along the lines, in exactly $mn - 1$ breaks.

Proof. Let $P(m, n)$ be the statement that an $n \times m$ bar can be broken into 1×1 pieces in $mn - 1$ breaks.

Base case: If $m = n = 1$, then no breaks are required, and $1 \cdot 1 - 1 = 0$.

Inductive step: Fix $m, n \geqslant 1$, and assume that $P(k, \ell)$ holds for all $1 \leqslant k \leqslant m$ and $1 \leqslant \ell \leqslant n$. We will show $P(m+1, n)$ and $P(m, n+1)$ individually.

To show $P(m+1, n)$, first make a break along a column into two pieces—am $m_1 \times n$ and an $m_2 \times n$ piece, with $1 \leqslant m_1, m_2 \geqslant m$ and $m_1 + m_2 = m + 1$. So, by the (strong) induction hypothesis, $P(m_1, n)$ and $P(m_2, n)$ both hold. So we can break the two pieces in $m_1 n - 1$ and $m_2 n - 1$ breaks, respectively, totaling

$$m_1 n - 1 + m_2 n - 1 + 1 = (m_1 + m_2)n - 1 = (m+1)n - 1$$

moves in total. Showing $P(m, n+1)$ follows similarly.

So by strong induction, $P(m, n)$ holds for all $m, n \geqslant 1$.

You try: Use strong induction to show the following claims.

1. Every amount of postage that is at least 12 cents can be made from 4-cent and 5-cent stamps.
2. In the game Nim, there are two players and two piles of matches. At each turn, a player removes some (non-zero) number of matches from one of the piles. The player who removes the last match wins.
   Claim: If the two piles contain the same number of matches at the start of the game, then the second player can always win.

Introduction to number theory

An integer a *divides* the integer b, written as $a|b$, if there exists an integer k such that $b = ka$:

$$(a|b) \Leftrightarrow \exists k \in \mathbb{Z}(b = ka).$$

If $a|b$, we call a a *divisor* of b.
If a is not a divisor of b, we write $a \nmid b$ (LaTeX: \nmid).

Examples:

1. Since $6 = 2 \cdot 3$, we have $2|6$ and $3|6$.
2. The divisors of 4 are $1, 2, 4, -1, -2$, and -4:
$$4 = 1 \cdot 4 = (-1)(-4) = 2 \cdot 2 = (-2)(-2).$$
3. The divisors of -4 are also $1, 2, 4, -1, -2$, and -4:
$$4 = 1(-4) = (-1)4 = 2(-2).$$
4. The divisors of 1 are 1 and -1.
5. Every integer $k \in \mathbb{Z}$ is a divisor of 0 since $k \cdot 0 = 0$.
6. Zero is only a divisor of itself, i.e. $0 \nmid k$ for all $k \in \mathbb{Z}_{\neq 0}$.

Theorem. Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $a|c$, then $a|(mb + nc)$, for all integers m and n.

Proof. If $a|b$ and $a|c$, then there exist $k, \ell \in \mathbb{Z}$ such that

$$b = ka \quad \text{and} \quad c = \ell a.$$

So

$$mb + nc = m(ka) + n(\ell a) = (mk + n\ell)a.$$

So since $mk + n\ell \in \mathbb{Z}$, we have $a|(mb + nc)$, as desired. □

You try: Let $a, b, c \in \mathbb{Z}$. Prove the following two claims.

Claim 1: If a divides b, then a divides b^2.

Claim 2: If $a|b$ and $b|c$, then $a|c$.

Hint: for each, if $x|y$, the first thing you want to try is writing "there exists $z \in \mathbb{Z}$ such that $xz = y$."

The greatest common divisor of two non-zero integers a and b, denoted $\gcd(a,b)$, is the largest positive integer that divides both numbers:

$$\Big(\gcd(a,b) = D\Big) \Leftrightarrow \Big((d|a \wedge d|b) \Rightarrow d \leqslant D\Big).$$

Examples:

$$\gcd(12,18) = 6, \quad \gcd(12,-18) = 6,$$
$$\gcd(-12,-19) = 6, \quad \gcd(12,35) = 1.$$

Note, for all non-zero integers a and b, we have $\gcd(a,b) > 0$.

If $\gcd(a,b) = 1$, we say a and b are relatively prime.