Cancellation law: We will prove by induction in $K \in \mathbb{N}$ that

$$m+K = n+K \Rightarrow m = n \quad \forall\, m, n \in \mathbb{N}.$$

For $K=1$, note that if $m+1 = n+1$, then

$$s(m) = m+1 = n+1 = s(n)$$

As s is injective, then $m = n$.

Now, suppose it holds for K (base of induction).

Let m, n, K be such that $m+(K+1) = n+(K+1)$.

Then,

$$\begin{aligned} s(m+K) &= m + s(K) \\ &= m + (K+1) \\ &= n + (K+1) \\ &= n + s(K) \\ &= s(n+K) \end{aligned}$$

As s is injective, we have $m+K = n+K$

By induction, we have $m = n$

Definition (Order) Given $m, n \in \mathbb{N}$, we say that $m < n$ if there exists $K \in \mathbb{N}$ such that $n = m+K$.

We say that $m \leq n$ if $m < n$ or $m = n$.

Facts about order:

(a) If $m < n$ and $n < r$, then $m < r$.

(b) Given $m, n \in \mathbb{N}$, exactly one of the following statements are true:

① $m < n$ ② $n < m$ ③ $n = m$

(c) If $m < n$, then $m+p < n+p \quad \forall\, p \in \mathbb{N}$.

(d) There are no $m, K \in \mathbb{N}$ such that $m < K < m+1$.

All these facts can be proven using the definition of order and the properties we have for $\mathbb{N}$. We will prove only the last one and leave the others as an exercise.

Proof of (4): First, we show the fact for $m=1$:

Claim: There is no $k \in \mathbb{N}$ such that $1 < k < 1+1 = 2 = s(1)$

proof: Suppose for contradiction that there exists $k \in \mathbb{N}$ such that $1 < k < 2$. Then, $\exists\, r \in \mathbb{N}$ such that $k = s(r) = r+1$ (every number $\neq 1$ is successor of someone).

As $k < 2$, $\exists\, p \in \mathbb{N}$ such that $2 = k+p$, and hence

$$2 = k+p = (r+1)+p = r+(1+p) = r+(p+1) = s(r+p)$$

This implies $s(1) = 2 = s(r+p)$, and hence $1 = r+p$.
Now, observe that we cannot have $1 = r+p$. In fact, if $p=1$, then we have $1 = r+p = r+1 = s(r)$, which is a contradiction.
If $p \neq 1$, then $\exists\, t \in \mathbb{N}$ with $p = s(t)$. This implies $1 = r+p = r+s(t) = s(r+t)$, which is a contradiction.
This finish the proof of the claim ——— ∎

Now, suppose that the statement holds for $m \in \mathbb{N}$.
Suppose for contradiction that it does not hold for $m+1$.
Then, $\exists\, k \in \mathbb{N}$ such that $m+1 < k < (m+1)+1 = m+2$

$m+1 < k \Rightarrow k = (m+1)+p$ for some $p \in \mathbb{N}$.

$k < m+2 \Rightarrow m+2 = k+r$, for some $r \in \mathbb{N}$.

Thus,

$$\begin{aligned} m+2 &= k+r \\ &= ((m+1)+p)+r \\ &= (m+1)+(p+r) \\ &= m+(1+(p+r)) \end{aligned}$$

By the cancelling law, we obtain

$$\begin{aligned} 2 &= 1+(p+r) \\ &= (1+p)+r \\ &= (p+1)+r \\ &= s(p+r) \end{aligned}$$

As $2 = S(1)$, we obtain $1 = p+r$ (recall that S is injective)

This is a contradiction. As we observed before, 1 cannot be written as the sum of two natural numbers ——————— ☐

Well-ordering principle: Let $A \subseteq \mathbb{N}$ be a non-empty subset. There exists $n_0 \in A$ such that $\{m : m < n_0\} \cap A = \emptyset$. The element n_0 is called the minimum element of A.

Proposition: The axiom of induction implies the well-ordering principle.

proof: For $n \in \mathbb{N}$, let $I_n := \{k \in \mathbb{N} : k \leq n\}$.

Suppose for contradiction that there exists a set $A \subseteq \mathbb{N}$ which does not have a minimum element, with $A \neq \emptyset$.

Let $B = \{n \in \mathbb{N} \mid I_n \cap A = \emptyset\}$.

If $n \in B$, then $I_n \cap A = \phi$. This implies $n \notin A$. Therefore, $B \subseteq \mathbb{N} \setminus A$

Observe that $1 \notin A$, as 1 is the smallest element in $\mathbb{N}$.

This implies that $1 \in B$.

If $n \in B$, then $I_n \cap A = \phi$. As $I_{n+1} = I_n \cup \{n+1\}$

(because there is no element in between n and $n+1$),

we have two choices

- $n+1 \in A$, and hence $n+1 = \min(A)$, contradiction.
- $n+1 \notin A$, and hence $I_{n+1} \cap A = \phi$, where $n+1 \in B$.

Therefore, $n \in B \Rightarrow n+1 \in B \quad \forall n \in \mathbb{N}$.

We conclude that $B = \mathbb{N}$. As $B = \mathbb{N} \setminus A$, we have

$A = \phi$, a contradiction. ∎

Proposition: the well-ordering principle implies mathematical induction.