I will start by reviewing a property of the set of natural number $\mathbb{N}$.

Note: $\mathbb{N} := \{ n \text{ integer} \mid n \geq 0 \}$. In particular $0 \in \mathbb{N}$.

We'll use this property to prove the division algorithm, first for integers (i.e. for $\mathbb{Z}$), then for polynomials ...

Well ordering principle: Any nonempty subset of $\mathbb{N}$ has the least element.

Compare: $(0,1) \subseteq \mathbb{R}$ is nonempty, and there is no "least element"

Well ordering principle is equivalent to induction:

Recall:

Principle of mathematical induction (PMI):

Suppose $S \subseteq \mathbb{N}$ has two properties:

(i) $0 \in S$

(ii) if $n \in S$ then $n+1 \in S$

Conclusion: $S = \mathbb{N}$.

Remark: PMI is often stated as:

PMI 2: Let $P_1, P_2, \ldots P_n \ldots$ be a collection of statements so that

i) P_1 is true

ii) if P_k is true then P_{k+1} is true.

Conclusion: P_n is true for all $n \geq 1$.

We'll see: PMI $\Leftrightarrow$ PMI 2.

Hence: (*) Well ordering $\Leftrightarrow$ PMI $\Leftrightarrow$ PMI 2

I'm going to jump ahead to the division "algorithm" and come back (*) later.

<u>Recall</u> An integer b <u>divides</u> $c \in \mathbb{Z}$ (we write $b \mid c$) if $c = bk$ for some $k \in \mathbb{Z}$

<u>Ex</u> $3 \mid 6$ since $6 = 2 \cdot 3$

$3 \nmid 7$ since $\nexists k$ s.t. $7 = 3k$

$n \mid 0$ $\forall n$ since $0 = 0 \cdot n$. . . .

"<u>Division algorithm" for $\mathbb{Z}$</u> For any two integers a, d with $d \geq 1$ there exist <u>unique</u> integers q, r so that

1) $a = q \cdot d + r$ $\qquad q$ = quotient

2) $0 \leq r < d$ $\qquad r$ = remainder.

<u>Proof</u> (existence) Idea: r is the smallest nonnegative integer so that $r = a - q \cdot d$ for some $q \in \mathbb{Z}$.

So let $S = \{a - td \mid t \in \mathbb{Z} \quad a - t \cdot d \geq 0\}$

<u>Note:</u> $S \neq \emptyset$: If $a \geq 0$, $a - 0 \cdot d \in S$.

If $a < 0$, $a - a \cdot d = a \cdot (1-d) \geq 0$ since $1-d, a \leq 0$.

By well-ordering principle S has the smallest element. So let $r = \min(S) = \min\{a - td \mid t \in \mathbb{Z}, a - t \cdot d \geq 0\}$

Then (i) $r \geq 0$ and (ii) $r = a - q \cdot d$ for some $q \in \mathbb{Z}$

We now argue that $r < d$.

Suppose not: $r \geq d$. Then

$0 \leq r - d = (a - q \cdot d) - d = a - (q+1)d$

Since $a - (q+1)d \geq 0$, $a - (q+1)d \, (= r - d) \in S$.

But $r - d < r$ (since $d \geq 1$). This contradicts $r = \min S$

<u>Conclusion:</u> $\exists q, r \in \mathbb{Z}$ s.t. $a = q \cdot d + r$ and $0 \leq r < d$.

(Uniqueness) Suppose $\exists q_1, q_2 \in \mathbb{Z}$, $r_1, r_2 \in \mathbb{Z}$ s.t.

$a = q_1 \cdot d + r_1 = q_2 \cdot d + r_2$ and $0 \leq r_1, r_2 < d$

May assume: $r_1 \le r_2$. Then

$0 \le r_2 - r_1 = (a - q_2 d) - (a - q_1 d) = (q_1 - q_2)\cdot d$

Since $r_2 < d$ and $r_1 \ge 0$, $r_2 - r_1 < d$ as well, ie

$$0 \le (q_1 - q_2)\cdot d < d$$

This can only happen if $q_1 - q_2 = 0$ (since $q_1 - q_2$, d are integers and $d > 0$).

$$\Rightarrow \quad r_2 - r_1 = 0 \quad \text{and} \quad q_1 - q_2 = 0$$

That is, $r_2 = r_1$ and $q_2 = q_1$. ☐

Theorem TFAE (The Following Are Equivalent)

1) Well-ordering principle: any $\emptyset \ne X \subseteq \mathbb{N}$ has the smallest element
2) PMI1: if $S \subseteq \mathbb{N}$, $0 \in S$ and $n \in S \Rightarrow n+1 \in S$, then $S = \mathbb{N}$.
3) PMI2: $\{p_n\}_{n \ge 1}$ collection of statements so that p_1 is true and (p_k true $\Rightarrow$ p_{k+1} true). Then p_n is true for all $n \ge 1$.

Proof (1) $\Rightarrow$ (2). Suppose $S \subseteq \mathbb{N}$, $0 \in S$, $n \in S \Rightarrow n+1 \in S$ and $S \ne \mathbb{N}$. Then $X = \mathbb{N} \setminus S := \{n \in \mathbb{N} \mid n \notin S\} \ne \emptyset$. By assumption X has the smallest element; call it k. $k \ne 0$ since $0 \in S$. So $k > 0$.
$\Rightarrow 0 \le k-1 < k$. Since $k-1 < k = \min X$, $k-1 \notin X$. $\Rightarrow k-1 \in S$
By assumption on S, $k = (k-1)+1 \in S$ as well. Contradiction since $k \in X = \mathbb{N} \setminus S$.

(2) $\Rightarrow$ (3) (ie, PMI1 $\Rightarrow$ PMI2) Let $\{p_n\}_{n \ge 1}$ be a collection of statements st p_1 is true and (p_k true $\Rightarrow$ p_{k+1} true) for all k.
Let $S = \{k \in \mathbb{N} \mid p_{k+1} \text{ is true}\}$. Then since $p_1 = p_{0+1}$ is true, $0 \in S$.
If $n \in S$ then p_{n+1} is true. Hence p_{n+2} is true. $\Rightarrow n+1 \in S$
By PMI 1, $S = \mathbb{N}$. $\Rightarrow$ p_{k+1} is true for all $k \ge 0$, ie PMI2 holds

(3) $\Rightarrow$ (1). Suppose $\phi \neq X \subseteq \mathbb{N}$ and X has no smallest element.

Let p_n = " $X \cap \{0, \ldots, n-1\} = \emptyset$ ", ie $0, 1, \ldots n-1 \notin X$.

Since X has no smallest element $0 \notin X$. $\Rightarrow p_1$ is true.

Suppose p_k is true: $X \cap \{0, \ldots k-1\} = \emptyset$.

If $k \in X$, then k is the smallest element of X (since $0, \ldots k-1 \notin X$).

But X has no smallest element. $\Rightarrow k \notin X$. $\Rightarrow p_{k+1}$ is true.

Therefore by PMI 2, p_n is true for all n

$\Rightarrow X = \phi$. contradiction.