Theorem 21 For all integers a and b with $b > 0$, there exist unique integers q and r such that $a = bq + r$, and $0 \leq r < b$.

Proof: Let $a = -5$ and $b = 2$. Then,

$$-5 = 2 \times (-3) + 1$$

So, for $a = -5$ and $b = 2$, there exists a unique q and r belonging to the set of integers such that $a = 2q + r$ with $0 \leq r < 2$ (i.e., $r = 0$ or 1).

By, theorem 16, every integer is either odd or even.

Corollary 1 For any integer a, b with $b > 1$, there exists a unique r $\in \mathbb{Z}$

Such that a = r (mod b) and $0 \leq r < be$

When $b = 3$, for any $z \in \mathbb{Z}$, there exists a unique integer r such that $a \equiv r \pmod 3$ and $r \in \{0, 1, 2\}$.

Theorem 21 For every integer n, $n^3 = n(mod 3)$
Proof: By corollary 1, we only have one of the three cases
Case 1: n = 0 (mod 3)

$$n^3 \equiv n \pmod 3 \longrightarrow 3 \mid (n^3 - n)$$
$$3 \mid (n^3 - n) \longrightarrow (n)(n-1)(n-1)$$
$$\text{By theorem 20, we will have } n^3 = 0^3 \pmod 3$$

Remark:
By reflexivity, $a \equiv b \text{ (mod } n) \longrightarrow b \equiv a \pmod n$.
Case 2: n = 1 (mod 3)
$n = 1(mod3)$, By theorem 20, $n^3 = 1^3(mod3)$
Similarly, $n = n^3(mod3)$
Case 3: n = 2 (mod 3)

Theorem 19 Let n belong to Z, Then n is even if and only if n^2 is even. Similarly, n is odd if and only if n^2 is odd.

Proof:

$\longrightarrow$

Suppose, n is even. Goal: n^2 is even.

Then n = 2k for some k in Z.

So, $n^2 = (2k) * n = 2(kn)$, where kn is in Z by the closure of Z

Hence n^2 is even.

$\longleftarrow$

Need to prove: if n^2 is even, then n is even.

$(P \implies Q) \equiv (\neg Q \implies \neg P)$

Contrapositive:

If n is not even, then n^2 is not even.

By theorem 16. If an integer is not even, then it is odd.

Suppose n is odd. THen n = 2k + 1 for some k in Z.

$$\text{So } n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

$$\text{Since } 2k^2 + 2k \in \mathbb{Z},\ n^2 \text{ is odd.}$$

Revisit Let $x \in \mathbb{R}$. We say x is rational if there exist integers p and q with $q \neq 0$ such that $x = \frac{p}{q}$. We say x is irrational if it is not rational.

Theorem 17: $\sqrt{2}$ is not rational.

Proof:

There exist $p, q \in \mathbb{Z}$ such that $\sqrt{2} = \frac{p}{q}$, $q \neq 0$.
$2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2$
$\Rightarrow p^2$ is even
$\Rightarrow p$ is even ($p = 2k$, where $k \in \mathbb{Z}$)
$\Rightarrow 2q^2 = (2k)^2 = 4k^2$.
$q^2 = 2k^2$
$\Rightarrow q^2$ is even
$\Rightarrow q$ is even ($q = 2L$, where $L \in \mathbb{Z}$)
$\sqrt{2} = \frac{p}{q}$ p is negative and -p is positive.

Rewriting:

Assume p is positive (if -p negative, we have $\sqrt{2} = \frac{-p}{-q}$ so we choose -p)
Consider $S = \{p \in \mathbb{Z}^+ | \sqrt{2} = \frac{p}{q} \text{ for } q \in \mathbb{Z}, q \neq 0\}$.
Note $S = \varnothing$. Then by the well-ordering property.
S has a smallest element p_0 such that $\sqrt{2} = \frac{p_0}{q_0}$ for some $q_0 \in \mathbb{Z}$, $q_0 \neq 0$,
where p_0 is p not p subscript 0.
Then $2 = \frac{p_0^2}{q_0^2}$ so $2q_0^2 = p_0^2$, which implies p_0^2 is even.
By Theorem 19, p_0 is even, so $p_0 = 2k$ for some $k \in \mathbb{Z}$.
$\Rightarrow 0 < k < p_0$
Plug it into our original equation to have:
$2q_0^2 = (2k)^2 = 4k^2 \Rightarrow q_0^2 = 2k^2$
So, q_0^2 is even. By Theorem 19, q_0 is even.
This implies $q_0 = 2L$ for some $L \in \mathbb{Z}$
Then $\sqrt{2} = \frac{p_0}{q_0} = \frac{2k}{2l} = \frac{k}{l} \Rightarrow k \in S$.
Since $k < p_0$, we have a contradiction.
Hence, $\sqrt{2}$ is not rational.
$\square$

Remark: We use proof by contradiction, then we prove that the well ordering property is contradicted