1 Introduction

Theorem 1.1. *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 1.1.1. *For any integer a, b with $b > 1$, there exists a unique $r \in \mathbb{Z}$ such that $a = r \pmod{b}$ and $0 \leq r < b$.*

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 1.2. *For every integer n, $n^3 \equiv n \pmod 3$.*

Proof: By Corollary 1, we only have one of the three cases:

Case 1: $n \equiv 0 \pmod 3$

$$n^3 \equiv n \pmod 3 \longrightarrow 3 \mid (n^3 - n)$$
$$3 \mid (n^3 - n) \longrightarrow (n)(n-1)(n-1)$$

By Theorem 20, we have $n^3 \equiv 0^3 \pmod 3$.

Case 2: $n \equiv 1 \pmod 3$

Similarly, $n = n^3 \pmod 3$.

Case 3: $n \equiv 2 \pmod 3$

$\square$

Theorem 1.3. *Let $n \in \mathbb{Z}$. 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 $k \in \mathbb{Z}$.
So, $n^2 = (2k) \times n = 2(kn)$, where $kn \in \mathbb{Z}$ by the closure of $\mathbb{Z}$.
Hence, n^2 is even.
$\longleftarrow$
Need to prove: if n^2 is even, then n is even.
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 $k \in \mathbb{Z}$.

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

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

2 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 2.1. $\sqrt{2}$ *is irrational.*

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. $\square$

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