Warm-Up: Make $+$ and $\cdot$ tables for arithmetic modulo 3.

Thm: Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. If

$$a \equiv b \mod m$$

then

$$a^n \equiv b^n \mod m$$

for every $n \in \mathbb{N}$.

Proof: Let $P(n)$ be "$a^n \equiv b^n \mod m$."
We'll use induction.

Base Case: $P(1)$ is given.

Inductive Step: Let $n \in \mathbb{N}$ and suppose $P(n)$ is true. That is, $a^n \equiv b^n \mod m$.

Since $a \equiv b \mod m$, we get

$$a^n \cdot a \equiv b^n \cdot b \mod m,$$

i.e., $a^{n+1} \equiv b^{n+1} \mod m$. So $P(n+1)$ is true.

Thus, $P(n)$ is true for all $n \in \mathbb{N}$ by P.M.I. ∎

Ex: What is the remainder when 91^{100} is divided by 3?

Since $91 \equiv 1 \mod 3$, we have

$$91^{100} \equiv 1^{100} \mod 3$$
$$\equiv 1 \mod 3.$$

So the remainder is 1.

Ex: What is the remainder when 257^{50} is divided by 5?

Since $257 \equiv 2 \mod 5$, we have

$$257^{50} \equiv 2^{50} \mod 5.$$

Now, $2^4 = 16$, so $2^4 \equiv 1 \mod 5$.

Write

$$50 = 4 \cdot 12 + 2. \quad \text{(50 divided by 4)}$$

Then

$$2^{50} = 2^{4 \cdot 12 + 2} = (2^4)^{12} \cdot 2^2,$$

So

$$
\begin{aligned}
257^{50} &\equiv 2^{50} \\
&\equiv (2^4)^{12} \cdot 2^2 \quad \text{mod } 5 \\
&\equiv 1^{12} \cdot 4 \quad \text{mod } 5 \\
&\equiv 4 \quad \text{mod } 5 .
\end{aligned}
$$

The remainder is 4.

Primes Redux

Thm: Every $n \in \mathbb{N}$ such that $n \geq 2$ is either a prime or a product of primes.

Proof #1: Suppose, to get a contradiction, that the theorem is false.

Let S be the set of all counterexamples, i.e. $n \in S$ if and only if $n \geq 2$ and n is not prime and n is not a product of primes.

Since S is not empty, by the Well-Ordering Axiom, there is a least element in S. Call it a.

Since $a \geq 2$, a is either prime or composite.

- If a is prime, then $a \notin S$, a contradiction.

- If a is composite, then $a = dk$ for some $d, k \in \mathbb{N}$ such that $2 \leq d \leq a-1$ and $2 \leq k \leq a-1$.

Thus, $d, k \notin S$, so d and k are each prime or products of primes. Then so is $a = d \cdot k$, implying $a \notin S$, a contradiction. ∎

To prove this without contradiction, we use a version of induction.

Idea: Let $P(n)$ be the sentence

"n is either a prime or a product of primes"

Base Case: $P(2)$ ✓ (2 is prime)

Inductive Step: $P(n) \Rightarrow P(n+1)$ ✗

The factorization of n has nothing to do with the factorization of $n+1$.

Instead, let

$$Q(n) = P(2) \wedge P(3) \wedge \cdots \wedge P(n)$$

<u>Base Case</u>: $Q(2) = P(2)$ ✓ (unchanged)

<u>Inductive Step</u>: $\underbrace{Q(n)}_{\substack{P(2),\ldots,P(n) \\ \text{all true}}} \Rightarrow \underbrace{Q(n+1)}_{\substack{P(2),\ldots,P(n),\, P(n+1) \\ \text{all true}}}$

✓ by assumption

So to prove $P(n+1)$, we get to use any and all previous cases.

<u>Proof #2</u>: Complete (strong) induction.

<u>Base Case</u>: 2 is prime. ✓

<u>Inductive Step</u>: Assume $2, 3, \ldots, n$ are each prime or a product of primes.

We must prove $n+1$ is also.

Case 1: $n+1$ is prime. ✓

Case 2: $n+1$ is composite.

Then $n+1 = d \cdot k$ for some $d, k \in \mathbb{N}$ with $2 \leq d, k \leq n$.

Thus, d and k are each primes or products of primes, so $n+1 = d \cdot k$ is a product of primes.

This completes the inductive step. By (complete) induction, every integer $n \geq 2$ is prime ~~or~~ a product of primes.

∎