Warm-Up: Make + and · tables for arithmetic modulo 4.

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 92^{100} is divided by 3?

Similarly, $92 \equiv 2 \mod 3$, so

$$92^{100} \equiv 2^{100} \mod 3.$$

Now, $2^2 \equiv 1 \mod 3$, so

$$2^{100} \equiv (2^2)^{50} \mod 3$$
$$\equiv 1^{50} \mod 3$$
$$\equiv 1 \mod 3.$$

Thus, the remainder is 1.

Ex: What is the remainder when 258^{50} is divided by 5?

Since $258 \equiv 3 \mod 5$, we have

$$258^{50} \equiv 3^{50} \mod 5.$$

Now, $3^4 = 81$, so $3^4 \equiv 1 \mod 5$.

Write

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

Then

$$3^{50} = 3^{4 \cdot 12 + 2} = (3^4)^{12} \cdot 3^2,$$

So

$$\begin{aligned} 258^{50} &\equiv 3^{50} \\ &\equiv (3^4)^{12} \cdot 3^2 \mod 5 \\ &\equiv 1^{12} \cdot 9 \mod 5 \\ &\equiv 4 \mod 5. \end{aligned}$$

The remainder is 4.

Primes Redux

Our goal is now to prove that every $n \in \mathbb{N}$ has a unique prime factorization.

Ex: $12 = 2^2 \cdot 3$

$55 = 5 \cdot 11$

$140 = 2^2 \cdot 5 \cdot 7$

Minor issue #1: 1 is not a product of primes.

Solution: Ignore 1.

(Or view it as the "empty product.")

Minor issue #2: What do we mean by "unique"?

Ex: $140 = 2 \cdot 2 \cdot 5 \cdot 7 = 2 \cdot 5 \cdot 2 \cdot 7 = 7 \cdot 2 \cdot 5 \cdot 2 = \cdots$

Solution: The factorization is unique up to reordering.

Or, unique if we list the primes in increasing order.

Thm (Fundamental Theorem of Arithmetic)

① Every $n \in \mathbb{N}$ such that $n \geq 2$ a product of primes.

② Every $n \in \mathbb{N}$ such that $n \geq 2$ can be written uniquely as a product of primes, in the following sense: Suppose that

$$n = p_1 p_2 \cdots p_r \quad \text{and} \quad n = q_1 q_2 \cdots q_s,$$

where $p_1, p_2, \ldots, p_r$ and $q_1, q_2, \ldots, q_s$ are all primes such that

$$p_1 \leq p_2 \leq \cdots \leq p_r \quad \text{and} \quad q_1 \leq q_2 \leq \cdots \leq q_s.$$

Then $r = s$ and $p_i = q_i$ for all $1 \leq i \leq r$.

We'll prove this soon.