Warm-Up: Make + and $\cdot$ 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 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

$$50 = 4 \cdot 12 + 2.$$ (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

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

<u>Ex</u>: $12 = 2^2 \cdot 3$
$55 = 5 \cdot 11$
$140 = 2^2 \cdot 5 \cdot 7$

<u>Minor issue #1</u>: 1 is not a product of primes.

<u>Solution</u>: Ignore 1.
(Or view it as the "empty product.")

<u>Minor issue #2</u>: What do we mean by "unique"?

<u>Ex</u>: $140 = 2 \cdot 2 \cdot 5 \cdot 7 = 2 \cdot 5 \cdot 2 \cdot 7 = 7 \cdot 2 \cdot 5 \cdot 2 = \cdots$

<u>Solution</u>: The factorization is unique <u>up to reordering</u>.
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.

Applications of FTA

In practice, finding the prime factorization is **HARD**.

But the FTA has many "applications" in theoretical math.

In particular, we can re-cast statements about divisibility in terms of prime factorizations.

Let $a, b \geq 2$ be integers.

- For any prime p,

  $p \mid a \iff$ p appears in the prime factorization of a

- $a \mid b \iff$ every prime in the prime factorization of a appears at least as many times in the prime factorization of b.

- The prime divisors of $\gcd(a,b)$ are the prime divisors that a and b have in common.

  The number of times a prime p appears in the factorization of $\gcd(a,b)$ is the smaller of

  - the number of times p appears in the factorization of a
  - " " " " " b

- $\gcd(a,b)=1 \iff a$ and b have no prime divisors in common

  "a and b are relatively prime"

Ex: $a = 96 = 2^5 \cdot 3 \cdot 5^0$, $b = 180 = 2^2 \cdot 3^2 \cdot 5$

$\gcd(96,180) = 2^2 \cdot 3 = 12$

We can compute the least common multiple (HW 12) similarly:

$\operatorname{lcm}(96,180) = 2^5 \cdot 3^2 \cdot 5 = 1440$