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

Thm (Division by a prime): Let p be a prime number. Then for all $x, y \in \mathbb{Z}$, if $p \mid xy$ then $p \mid x$ or $p \mid y$.

i.e.,

$$xy \equiv 0 \bmod p \Rightarrow \begin{matrix} x \equiv 0 \bmod p \\ \text{or} \\ y \equiv 0 \bmod p \end{matrix}$$

Note: The requirement that p be prime is important!

Ex: $4 \mid 6 \cdot 10$ (since $6 \cdot 10 = 60 = 4 \cdot 15$), but $4 \nmid 6$ and $4 \nmid 10$.

Proof: Let p be a prime and $x, y \in \mathbb{Z}$. Suppose $p \mid xy$.

If $p \mid x$, then we are done. So suppose $p \nmid x$. We must show that $p \mid y$.

Since $p \nmid x$, $\gcd(p, x) = 1$ (HW 13).

Thus, by the reverse Euclidean Algorithm, there exist $u, v \in \mathbb{Z}$ such that

$$pu + xv = 1$$

Multiply by y to get

$$puy + xyv = y$$

Since $p \mid puy$ and $p \mid xyv$, we have $p \mid y$, as desired. $\blacksquare$

Cor: Let p be a prime. For each $n \in \mathbb{N}$ and all $x_1, x_2, \ldots, x_n \in \mathbb{Z}$, if $p \mid (x_1 x_2 \cdots x_n)$ then p divides at least one of $x_1, x_2, \ldots, x_n$.

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

"For all $x_1, \ldots, x_n \in \mathbb{Z}$, if $p \mid (x_1 \cdots x_n)$ then p divides at least one of the x_i."

We will prove $P(n)$ holds for all $n \in \mathbb{N}$ by induction.

Base Case: $P(1)$ is automatically true, since if $p \mid x_1$, then $p \mid x_1$

Inductive Step: Let $n \in \mathbb{N}$ and suppose $P(n)$ is true.

Let $x_1, \ldots, x_{n+1} \in \mathbb{Z}$ and suppose

$$p \mid (x_1 \cdots x_n) \cdot (x_{n+1}).$$

By the theorem on division by a prime, $p \mid (x_1 \cdots x_n)$ or $p \mid x_{n+1}$.

If $p \mid (x_1 \cdots x_n)$, then by $P(n)$, $p \mid x_i$ for some $1 \le i \le n$, and we have the desired conclusion.

If $p \mid x_{n+1}$, then we also have the desired conclusion.

In either case, $P(n+1)$ is true, completing the inductive step.

$\blacksquare$