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

i.e., $xy \equiv 0 \bmod p \Rightarrow$ $x \equiv 0 \bmod p$ or $y \equiv 0 \bmod p$

First:

<u>Lemma</u>: Let p be a prime and $x \in \mathbb{Z}$. If $p \nmid x$, then $\gcd(p, x) = 1$.

<u>Proof</u>: Let $d = \gcd(p, x)$. Then $d \in \mathbb{N}$ and $d \mid p$ and $d \mid x$.

Since $d \mid p$, either $d = 1$ or $d = p$. But $p \nmid x$, so it must be that $d = 1$. ∎

Proof of Theorem on Division by a prime:

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

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

Since $p \nmid x$, $\gcd(p, x) = 1$ by the Lemma.
Thus, there exist $u, v \in \mathbb{Z}$ such that

$$pu + xv = 1$$

Multiplying by y, we get

$$pyu + xyv = y.$$

Since $p \mid pyu$ and $p \mid xyv$ (because $p \mid xy$), we get $p \mid y$.

$\blacksquare$

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. ∎

Unique Factorization

We would like to say each $n \in \mathbb{N}$ has a unique prime factorization, i.e., n can be written as a product of primes in only one way.

Problem #1: 1 is not a product of primes

Solution: Ignore 1.
(Or, view 1 as the "empty product")

Problem #2: Commutativity.

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: Write the factors in increasing order.

Thm (Fundamental Theorem of Arithmetic)

① Every $n \in \mathbb{N}$ such that $n \geq 2$ is either a prime or 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 $1 \leq i \leq r$.

Proof: ① We proved this last time.

② Let $P(n)$ be "n can be written uniquely as a product of primes (with the factors listed in increasing order)."

We will prove $P(n)$ is true for all $n \geq 2$ by complete induction.

Base Case: $n = 2$. One factorization is

$$2 = 2.$$

Suppose $2 = p_1 p_2 \cdots p_r$ is any other factorization into primes with $p_1 \leq p_2 \leq \cdots \leq p_r$. Then, since $2 \leq p$ for every prime p, we must have

$$2 = p_1 p_2 \cdots p_r \geq 2^r,$$

so $r = 1$. Thus, $2 = p_1$, and this factorization is the one we already knew.

Inductive Step: Let $n \in \mathbb{N}$, $n \geq 2$, and assume $P(2), \ldots, P(n)$ are all true.

We prove $P(n+1)$ by considering two cases.

Case 1: $n+1$ is prime. Then any factorization

$$n+1 = p_1 p_2 \cdots p_r$$

into primes p_i with $p_1 \leq p_2 \leq \cdots \leq p_r$ must have $r = 1$ and $p_1 = n+1$.

Why? If $r \geq 2$, then

$$n+1 = a \cdot b$$

where $a = p_1 \neq 1$ and $b = p_2 \cdots p_r \neq 1$, contradicting that $n+1$ is prime.

So $P(n+1)$ is true in this case.

__Case 2__: $n+1$ is composite.

Suppose

$$n+1 = p_1 p_2 \cdots p_r \quad \text{with} \quad p_1 \leq p_2 \leq \cdots \leq p_r$$

and

$$n+1 = q_1 q_2 \cdots q_r \quad \text{with} \quad q_1 \leq q_2 \leq \cdots \leq q_s,$$

where all p_i and q_j are prime.

Since $n+1$ is not prime, $r \geq 2$ and $s \geq 2$.

Without loss of generality, we may assume

$$p_1 \leq q_1 .$$

Now, p_1 divides $n+1 = q_1 \cdots q_s$, so by the

Applies because – p_1 is prime

Corollary, p_1 divides one of the factors.

Say $p_1 \mid q_k$.

Since q_k is prime, its only positive divisors are 1 and itself.

Since $p_1 \neq 1$, it must be that $p_1 = q_k$.

Now, $p_1 \leq q_1 \leq q_k = p_1$,

so we must have equality throughout, and $p_1 = q_1$.

Therefore,

$$n+1 = p_1(p_2\cdots p_r) = q_1(q_2\cdots q_s)$$
$$= p_1(q_2\cdots q_s).$$

Cancelling $p_1 \neq 0$, we get

$$p_2\cdots p_r = q_2\cdots q_s. \quad (*)$$

Call this number ℓ. Then $2 \leq \ell \leq n$ (Why? $r \geq 2$ and $n+1 = p_1 \ell$), so $P(\ell)$ is true.

Since $(*)$ gives two factorizations of ℓ into prime factors listed in increasing order, $P(\ell)$ implies

- $r-1 = s-1$

and

- $p_i = q_i$ for all $2 \leq i \leq r$.

It follows that $r = s$ and $p_i = q_i$ for all $1 \leq i \leq r$, so $P(n+1)$ is true. ∎