Fundamental Theorem of Arithmetic

Let $n \geq 2$ be an integer.

1. n can be factored as a product of primes.

2. This factorization is unique.
   ↳ up to commutativity

We proved 1 last week.

The proof of 2 uses

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.,

$$xy \equiv 0 \bmod p \implies x \equiv 0 \bmod p \text{ or } y \equiv 0 \bmod p$$

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 15).

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. ∎

Proof of FTA part 2

Let $P(k)$ be the sentence

"Any integer $n \geq 2$ which is equal to a product of k primes has a unique prime factorization."

We will prove $P(k)$ is true for all $k \in \mathbb{N}$ by induction.

<u>Base Case</u>: $k=1$. If n is a product of one prime, then

$$n=p$$

is prime.

If $n=p=q_1 q_2 \cdots q_\ell$ is another factorization into primes q_i, then $p \mid q_1 \cdots q_\ell$, so by the corollary p divides one of the q_i.

WLOG, $p \mid q_1$. But p and q_1 are both prime, so $p=q_1$. If $\ell \geq 2$, then

$$\cancel{p} = \cancel{p} q_2 \cdots q_\ell$$

so

$$1 = q_2 \cdots q_\ell .$$

But this is impossible, so $\ell=1$ and

$$n=p$$

is the unique prime factorization. ∎

__Inductive Step:__ Let $k \in \mathbb{N}$ and suppose $P(k)$ is true.

Now, let $n \in \mathbb{N}$ be such that

$$n = p_1 p_2 \cdots p_{k+1}$$

is a product of $k+1$ primes p_i

If $n = q_1 q_2 \cdots q_\ell$ is another prime factorization, then since $p_1 | n$, we have $p_1 | (q_1 \cdots q_\ell)$.

Similar to above, we deduce that p_1 is equal to one of the q_i's. WLOG, $p_1 = q_1$.

Then $\cancel{p_1} p_2 \cdots p_{k+1} = \cancel{p_1} q_2 \cdots q_\ell$, so

$$p_2 \cdots p_{k+1} = q_2 \cdots q_\ell .$$

But the left-hand side is a product of k primes, so it has a unique prime factorization by $P(k)$.

Thus, $\ell = k+1$ and, up to reordering, the primes $q_2, \ldots, q_{k+1}$ are exactly the primes $p_2, \ldots, p_{k+1}$.

That is, n has a unique prime factorization.

This proves $P(k+1)$, completing the inductive step. ■

Sets

"Def": A set is an unordered collection of objects, called elements of the set.

Actual definition is a list of axioms

One way to describe a set: list its elements inside braces.

Ex: $\{1,2,3\}$, $\{$red, blue$\}$, $\{$☺, \$, ★, □$\}$ are sets

Important notes:

- The elements in a set are unordered. So

  $\{1,2,3\}$, $\{1,3,2\}$, $\{2,1,3\}$, $\{2,3,1\}$, $\{3,1,2\}$, $\{3,2,1\}$

  are six ways of writing the same set.

- The elements are distinct – no object can appear more than once. If we write

  $\{1,1,1,2,2,2,2,2,2,3,3\}$,

  this means the set $\{1,2,3\}$.