Warm-Up: Prove that $n! > 2^n$ for all integers $n > 3$ without induction.

Suppose not. Then there is a smallest integer $a > 3$ such that $a! \leq 2^a$. (why?)

What can you say about a?

Thm: Let $n \in \mathbb{N}$. If $n > 1$, then there is a prime p such that $p \mid n$.

Proof: Suppose, to get a contradiction, that the theorem is false.

That is, there is a natural number greater than 1 which is not divisible by any prime.

By the Well-Ordering Principle, there is a smallest such number. (Why?) Call it a.

So
- $a > 1$
- no prime divides a
- If $1 < n < a$, then n is divisible by some prime.

Now, a is prime or composite.

- If a is prime, then $a \mid a$, so a is divisible by a prime, which is a contradiction.

- If a is composite, then it has a positive divisor d with $d \neq 1$ and $d \neq a$.

  Since $d \mid a$, $d \leq a$. But $d \neq a$, so $d < a$.
  Also, $d \neq 1$, so $d > 1$.

Thus, d must have a prime divisor p.
Since $p \mid d$ and $d \mid a$, we have $p \mid a$. (HW 10)
This is a contradiction.

Thus, the theorem holds for all natural numbers $n \geq 2$.

∎

The infinitude of primes

Thm: There are infinitely many prime numbers.

Proof: Suppose, for the sake of contradiction, that there are only finitely many primes, say

$$p_1, p_2, \ldots, p_n.$$

Let $m = p_1 p_2 \cdots p_n$ be the product of all of these primes.

Now, by the previous theorem, there is a prime q such that $q \mid (m+1)$.

Since q must be one of the primes $p_1, \ldots, p_n$ (because these are the only primes), so $q \mid m$.
Thus, q divides

$$(m+1) - m = 1.$$

But this is a contradiction, since $q \geq 2$. ∎