**Warm-Up:** Prove that $1+3+5+\cdots+(2n-1)=n^2$ for each $n\in\mathbb{N}$, without using induction

Suppose not. Then there is a smallest $a\in\mathbb{N}$ such that $1+3+5+\cdots+(2a-1)\neq a^2$. (why?)

What can you say about $a$?

---

## Proof by "Smallest Counterexample"

Suppose we want to prove a statement of the form

$$(\forall n\in\mathbb{N})\,P(n). \qquad (\star)$$

One option is to use induction.

Alternatively, suppose $(\star)$ is false, to get a contradiction! Then

$$(\exists n\in\mathbb{N})\,\neg P(n),$$

so $P(n)$ is false for some $n$.

Let $a \in \mathbb{N}$ be the smallest such $n$. So

- $P(a)$ is false
- If $n \in \mathbb{N}$ and $n < a$, then $P(n)$ is true.

Now, try to leverage this into a contradiction.

Note: The number $a$ exists by the Well-Ordering property:

Let $S$ be the set of all $n \in \mathbb{N}$ such that $P(n)$ is false. $S$ is non-empty by our assumption that $(\star)$ is false, so it has a smallest element by Well-Ordering.

**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 $1 < d < a$, then $d$ 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 $n \geq 2$.

$\blacksquare$

# 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 $q \geq 2$. $\blacksquare$