Proof by Smallest Counterexample

Definitions:

- $\log_2(n)$ is x such that $2^x = n$.
  $\lfloor \log_2(n) \rfloor$ is the unique i s.t. $2^i \leq n < 2^{i+1}$

  e.g. $\lfloor \log_2(2) \rfloor = 1$, $\lfloor \log_2(3) \rfloor = 1$, $\lfloor \log_2(4) \rfloor = 2$
  $\lfloor \log_2(31) \rfloor = 4$, $\lfloor \log_2(32) \rfloor = 5$, $\lfloor \log_2(33) \rfloor = 5$

- Prime factorization of n is the representation of n as multiplication of a list of primes.
  e.g. $12 = 2 \times 2 \times 3$, $6! = 2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 5$

- Define $SIZE(n)$ to be the number of prime factors in prime factorization of n.
  e.g. $SIZE(12) = 3$, $SIZE(6!) = SIZE(720) = 7$

Proof by Smallest Counterexample

Theorem:
For any positive integer n, $SIZE(n) \leq \lfloor \log_2(n) \rfloor$.

Proof:
Let $P(n)$ be the statement $SIZE(n) \leq \lfloor \log_2(n) \rfloor$.
Assume the theorem is wrong.
i.e. There is a smallest integer m s.t. $P(m)$ is false.

Let p be a prime factor of m. Then,

$SIZE(m)$

$= SIZE(m/p \times p)$

$= SIZE(m/p) + 1$ By definition

$\leq \lfloor \log_2(m/p) \rfloor + 1$ $m/p < m$, so $P(m/p)$ is true.

$\leq \lfloor \log_2(m/2) \rfloor + 1$ By definition

$\leq \lfloor \log_2(m) \rfloor$ Contradiction!

Proof by Contradiction

Theorem:
There are infinitely many number of primes.

Proof:
Assume the number of primes is finite.
Let m be the largest prime. Consider $n = m! + 1$,
$n\ mod\ 2 = 1$
$n\ mod\ 3 = 1$
$n\ mod\ 5 = 1$
$\vdots$
$n\ mod\ m = 1$
$\Rightarrow$ No prime is a factor of n .
$\Rightarrow$ n is a prime greater than m. Contradiction!