Proposition There are infinitely many primes.

Proof: We will use proof by contradiction: Suppose there are only finitely many primes. In particular, assume there are precisely N primes and let $p_1, p_2, \ldots, p_N$ be our complete list of prime numbers.

Next, we consider the number $q = p_1 p_2 \cdots p_N + 1$. Notice that for all $1 \leq j \leq N$, $p_j > 1$ (since it's a prime). Also, for any particular $1 \leq \ell \leq N$, we then have that $p_1 p_2 \cdots p_N$ is a positive multiple of p_ℓ, so $q = p_1 p_2 \cdots p_N + 1 \geq p_\ell + 1 > p_\ell$. Therefore, q is bigger than any number on our list $p_1, \ldots, p_N$ (and consequently it is bigger than 1 as well).

Suppose that $q = ab$ for some natural numbers a and b. In addition, suppose that $a \neq 1$. Since $q > 1$, we have that both $a \neq 0$ and $b \neq 0$ (otherwise, we'd have that $q = ab = 0 < 1$). Thus $a > 1$ (since $a \neq 0, 1$). We have previously shown that any natural number bigger than 1 is a product of primes. Thus a must be divisible by at least one prime factor, say p is such a prime factor. Well, since p is prime, we must have that $p = p_k$ for some $1 \leq k \leq N$ (since $p_1, \ldots, p_N$ is a complete list of primes). Then p divides a and a divides q so that p must divide q. But $p = p_k$ is a factor of $p_1 p_2 \cdots p_N$, so p divides $p_1 p_2 \cdots p_N = q - 1$.

We now know that p both divides q and $q - 1$. Therefore, there exist n and m such that $q = pn$ and $q - 1 = pm$. This implies that $pn - 1 = q - 1 = pm$ so that $p(n - m) = pn - pm = 1$. However, notice that since 1 is positive, we cannot have $n - m \leq 0$ (since $p > 1$ this would give us $1 = p(n - m) \leq 0$). Thus $n - m > 0$. But then $n - m \geq 1$ so that $1 = p(n - m) \geq p \cdot 1 = p > 1$. Thus $1 > 1$. This is absurd (contradiction)!

Therefore, we cannot have that $a \neq 1$ (the last uncontradicted hypothesis we made). Thus if q factors, then one of those factors must be $a = 1$. This means that q is prime. But we already have that q is bigger than any prime on our list: $p_1, \ldots, p_N$. Therefore, our list is incomplete (contradiction). Thus no list of primes can be complete. This means we must have infinitely many primes. ■

Notice how our proof meanders around as we consider various possibilities. But as we consider these possibilities, we keep running into roadblocks. This is the nature of proof by contradiction: We try every possible road until we find that no road leads anywhere.

Warning: This proof does **not** say that given a list of primes $p_1, \ldots, p_N$, that $q = p_1 \cdots p_N + 1$ is also a prime. We could only get that q was prime using the (untrue) assumption that $p_1, \ldots, p_N$ was a complete list of primes. On the other hand, a careful reading of our proof reveals that if $q = p_1 \cdots p_N + 1$ isn't prime, then its prime factors must not appear on our list. In other words, the factorization of $q = p_1 \cdots p_N + 1$ does not involve any prime in the list $p_1, p_2, \ldots, p_N$.

It is interesting to note that this process of multiplying known primes together and adding one does generate some primes. For example: the empty product is defined to be 1, so the empty product (from an empty list of primes) plus 1 is 2 (prime). Now $2 + 1 = 3$ (prime). Next, $2 \cdot 3 + 1 = 7$ (prime). So far $2, 3,$ and 7 are all prime. Notice that we've already missed a prime (i.e., 5). Keep on going $2 \cdot 3 \cdot 7 + 1 = 43$ (still prime). But then this stops working: $2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807$ which is not a prime since $1807 = 13 \cdot 39$. As we noted from a careful reading of our proof, the factors of 1807 aren't on our list: $2, 3, 7, 43$.

If we try making our list by using *all* previous primes, this still doesn't work. Again, empty product$+1 = 2$, $2 + 1 = 3$, and $2 \cdot 3 + 1 = 7$ (all prime so far). Then $2 \cdot 3 \cdot 5 + 1 = 31$ (prime), $2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ (prime), and $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$ (prime). But $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30,031$ is not prime since $30,031 = 59 \cdot 509$. Again, notice that 59 and 509 were not (yet) part of our list.