THERE ARE INFINITELY MANY PRIME NUMBERS

Proof (long version). By contradiction.

Suppose that there are a finite number of primes. Then we can write them in a list: 2, 3, 5, 7, …, p_n, where p_n is the last prime number. Let $p_1 = 2$, $p_2 = 3$, and so on, so this list can just be written as $p_1, p_2, p_3, \ldots, p_{n-1}, p_n$.

Multiply all of the p_i together and add one, and call the result q:

$$q = p_1 \cdot p_2 \cdot p_3 \cdots p_{n-1} \cdot p_n + 1.$$

Then q is a positive integer greater than 2, so it's either prime or composite.

Clearly q is larger than any the primes in $p_1, p_2, \ldots p_n$, so it can't be somewhere on this list, i.e., q itself is not prime.

Therefore q must be composite: there is some prime number that divides evenly into q. Call this prime number P, and keep in mind that P must be somewhere on our list $p_1, p_2, \ldots, p_n$ since it is a list of all the prime numbers.

Since P is one of the p_i, it divides evenly into $p_1 \cdot p_2 \cdots p_n$.

Then in the equation

$$q = p_1 \cdot p_2 \cdot p_3 \cdots p_{n-1} \cdot p_n + 1,$$

P divides evenly into q and it divides evenly into $p_1 \cdot p_2 \cdot p_3 \cdots p_{n-1} \cdot p_n$, so it must divide evenly into 1 as well. But that is impossible! Since P is a prime number, it's greater than 1, so it cannot divide evenly into 1.

Therefore our original assumption, "there are a finite number of primes," is false. There are an infinite number of primes. □

Example: what if there were only two prime numbers? They would be 2 and 3. How would the above proof work out in this case?

Our list of primes is $p_1 = 2, p_2 = 3$. The number q is $q = 2 \cdot 3 + 1 = 6 + 1$. Then $q = 7$ is either prime or composite. It can't be prime—it's greater than 2 and it's greater than 3, and those are the only two primes (already you can see where only have two primes leads us). So it must be composite. Since it's composite, either 2 or 3 divides evenly into it.

Let's say 2 divides evenly into q. Then we can write $q = 2 \cdot Q$ (Q is just $q/2$). Notice that 2 also divides evenly into $2 \cdot 3$. Then in the equation

$$q = 2 \cdot 3 + 1,$$

divide everything by 2. You get

$$Q = 3 + \frac{1}{2}.$$

Since q is evenly divisible by 2, Q is a whole number. So on the left we have a whole number, on the right we have 3.5. These are clearly not equal, but they must be equal! This is a contradiction. Our assumption that there are only two primes led us to an impossible situation. (Instead of dividing everything by 2, we could have said something about 1 being divisible by 2, but it's essentially the same thing.)

The same thing would happen if instead we say that 3 divides evenly into q, we'd just get $Q = 2.33333$ which is also not a whole number.

You can do the same process for any finite number of primes that you want, it always leads to a contradiction.

This is the short version of the proof. Anything less detailed than this may not receive full credit on the exam.

Proof (short version). By contradiction.

Suppose that there are finitely many primes: $p_1, p_2, \dots, p_n$.

Define q as

$$q = p_1 \cdot p_2 \cdots p_n + 1.$$

Since q is greater than each prime number, it cannot be prime. Therefore q is composite. Since q is composite, some prime number P divides q.

Also, P divides $p_1 \cdot p_2 \cdots p_n$ since it is one of the primes.

Then P divides q and $p_1 \cdot p_2 \cdots p_n$, so P must divide 1 as well. This is a contradiction: P is prime, it cannot divide evenly into 1. Therefore the original assumption is false. There are infinitely many primes.

□