Infinity Of Primes

All letters will denote naturals that are : 1 , 2 , 3 , 4 , . .
If $a = bc$ then the b , c numbers are called dividers of a.
Every $a = 1 \cdot a$ and these two, the 1 and a dividers are called the trivial dividers of a.
If $a = bc$ with non trivial dividers, that is both b , c above 1 and under a then such product form is called a decomposition of a and a itself a composite.
The first few composites are : $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, $9 = 3 \cdot 3$, . . .
One or both members in a decomposition can again be composites and so then we can continue the decomposition. Above, 8 was the first such because it had the 4 composite member.
So the full decomposition of 8 is $2 \cdot 2 \cdot 2$. In such full decompositions we always get non composite final members above 1. So the non composites above 1 became called as primes.
The first few prime are: 2 , 3 , 5 , 7 , 11 , 13 , 17 , . . .
The larger than 1 dividers of an n are also called as factors of n.
So a prime is simply a number that has only itself as factor.
Also, a full decomposition can be called as a prime factorization.
The amazing fact is that regardless how we arrive to a prime factorization, the final prime factors will be the same. As an example, we show some prime factorizations of 60:

$$60 = \begin{cases} 2 \cdot 30 = \begin{cases} 2 \cdot 2 \cdot 15 = 2 \cdot 2 \cdot 3 \cdot 5 \\ 2 \cdot 5 \cdot 6 = 2 \cdot 5 \cdot 2 \cdot 3 \end{cases} \\ 5 \cdot 12 = \begin{cases} 5 \cdot 2 \cdot 6 = 5 \cdot 2 \cdot 2 \cdot 3 \\ 5 \cdot 3 \cdot 4 = 5 \cdot 3 \cdot 2 \cdot 2 \end{cases} \end{cases}$$

This claim is the Unique Prime Factorization Theorem or Fundamental Theorem Of Arithmetic.
Our subject, the infinity of primes, does not rely on this much harder provable fact.
It follows from the much more trivial fact that every number above 1 has prime factorization.
In fact, merely from the fact that every number above 1 has prime factor.
But to avoid the successive decomposition, we will show this in an other way now:
Every $n > 1$ has some factor since n itself is such.
So the F(n) set of all factors of any $n > 1$ number is never empty.
The smallest member of F(n) is denoted as minF(n).
We claim that minF(n) is always a prime.
First of all, $\text{minF}(n) > 1$ since all factors are above 1 by definition.
So we only must show that minF(n) is not composite, so it has no factor under itself.
And indeed, if it had an $f < \text{minF}(n)$ factor then f were factor of n too so it were contradicting that minF(n) is the smallest factor of n.
Let's regard the $n = p_1 p_2 \ldots p_m + 1$ value, using the $p_1 , p_2 , \ldots , p_m$ primes.
By our result then $\text{minF}(n) = \text{minF}(p_1 p_2 \ldots p_m + 1)$ is again a p prime but we now also know that it must be different from all the $p_1 , p_2 , \ldots , p_m$ primes.
Indeed, p divides n but neither of the $p_1 , p_2 , \ldots , p_m$ primes divide n since these have exactly 1 remainder if we divide $n = p_1 p_2 \ldots p_m + 1$ with either of them.
So $\text{minF}(p_1 p_2 \ldots p_m + 1)$ is a prime different from any of $p_1 , p_2 , \ldots , p_m$.
Thus we get instantly that there can not be only m many $p_1 , p_2 , \ldots , p_m$ primes.
If we don't want to use the minF(n) idea then we can still argue indirectly as follows:
Suppose there were only m many $p_1 , p_2 , \ldots , p_m$ primes.
The $p_1 p_2 \ldots p_m + 1$ number is not dividable by these, so it could not have any prime factor.
Strangely, this simplest argument was only recognized in the 19-th century by Kummer.
Our modernized argument was direct and an even more concrete one was already discovered by Euclid. As we'll see, the trick of multiplying all the primes and adding 1, was Euclid's.
We'll modernize Euclid's argument too by a smart definition as follows:
Let's call an n number k-undividable if neither of 2 , 3 , . . , k divides n.

Obviously, this is only possible if $k < n$ since n divides n.
Also observe that an n is prime if and only if it is $(n-1)$-undividable.
Let's denote the set of all k-undividable numbers as $U(k)$.
Now our first claim is that for every $k > 1$ there are k-undividable numbers.
So $U(k)$ is never empty if $k > 1$.
Let's form the $2 \cdot 3 \cdot 4 \cdot \ldots \cdot k = k!$ number also called as k factorial.
$k! + 1$ has 1 remainder to each of the $2, 3, \ldots, k$ numbers so it is indeed k-undividable.
Now let's abbreviate the smallest k-undividable number, that is $\min U(k)$ as k^*.
We claim that k^* is a prime and it is actually the first prime after k.
Suppose k^* had an f factor smaller than k^* itself.
First of all, every d divider of f is divider of of k^* too and so since k^* has no divider among $2, 3, \ldots, k$ thus neither has f.
So f were a k-undividable number too, contradicting that k^* was the smallest.
Now to see the second claim that k^* is the first prime after k:
If a p prime were such that $k < p < k^*$ then p were a k-undividable number under k^*, contradicting again the minimality of k^*.
As we see, both claims were shown indirectly but k^* itself is a concrete prime.
This at once implies that for every k number there is bigger prime and so indeed, there are infinite many primes.
The obvious question is how far can k^* be after k.
In other words, if there is some $f(k)$ function so that $k^* < f(k)$.
Of course k^* is itself a function or Euclid's construction gives one as $k! + 1$.
The first is not a concretely calculabe function from the basic operations while the second is huge compared to the observable k^* values.
The still quite weak $k^* < 2k$ result was only proved by Chebishev in the 19-th century.
This shows how difficult this next prime bounding is.
An other take on the same problem is bounding the gaps between the primes.
Let n_* denote the last prime up to n so allowing n itself if it is a prime.

Then $\delta(n) = n^* - n_*$ is the prime gap at n.

These gaps can be very big, in fact arbitrary big but even relative to n can vary a lot.
Chebishev was also the first to get exact results about the limit behavior of these gaps.
$\delta(n)$ is in average $\log(n)$ around n. This denotes logarithm with base $e = 2.718\ldots$
The base 10 logarithm is simply the number of 0-s in a 10 power and so to get a feel of the prime density is very easy by multiplying this 0 number by $\log(10) \approx 2.3$.
So for example, around one million, $\delta(1000{,}000) \approx 6 \times 2.3 \approx 14$ so in average, every 14-th number is a prime.
The meaning is clear but to tend both n and some surrounding to infinity is complicated and a simpler averaging would be to regard the δ values not around, rather up to n.
This average of course feels much smaller than an around average because the gaps are increasing. Surprisingly, the difference is only 1. So the average up to n is $\log(n) - 1$.

And if $\pi(n)$ denotes the number of primes up to n then this average is $\frac{n}{\pi(n)}$.

So the limit law is $\frac{n}{\pi(n)} \approx \log(n) - 1$. Amazingly, to prove this, it was enough to prove the consequence that the ratio of the two sides tends to 1 which is denoted by $\sim$.

This of course is true without the -1 part and so $\frac{n}{\pi(n)} \sim \log(n)$ or $\pi(n) \sim \frac{n}{\log(n)}$.

This is called the Prime Number Theorem, referring to the $\pi(n)$ number of primes as simply prime number. Now back from tendencies to actually limit the gaps:
A Conjecture of Cramer claims that: $n > 7 \rightarrow \delta(n) < (\log(n))^2$.
This also means that: $p \geq 11 \rightarrow p^* < p + (\log(p))^2$.
A consequence of this would be that: $p \geq 127 \rightarrow p^* < p + \sqrt{p}$.